Intego VirusBarrier X6 User Manual

Welcome to the User Manual for Intego VirusBarrier X6, the best antivirus for Mac. Use the Table of Contents below to go to the different sections of the manual. You can come back to this main Table of Contents at any time by clicking the *Go to Main Table of Contents* link at the top of each page.

For information about installing VirusBarrier X6 and updating the program and its filters with Intego NetUpdate, see the Intego Getting Started Manual.

Table of Contents

1. Welcome to VirusBarrier X6
2. Getting Started with Intego VirusBarrier X6
3. Protecting Your Mac from Viruses and Malware
4. Protecting Your Mac from Network Attacks
5. Using VirusBarrier X6 Monitoring Tools
6. VirusBarrier X6 Preferences and Configurations
7. Appendix: Creating Custom Firewall Rules

© 2011 Intego. All Rights Reserved.

Welcome to VirusBarrier X6

- About Intego VirusBarrier X6
- Installation
- Updating VirusBarrier X6 and Virus Definitions
- About Your Copy of Intego VirusBarrier X6
- Technical Support

Go to Main Table of Contents

About Intego VirusBarrier X6

VirusBarrier X6 is much more than just an antivirus. It's the only antivirus program for Mac that includes full anti-malware protection as well as a firewall and network-protection features. No other antivirus for Mac includes as many features as VirusBarrier X6.

While viruses, Trojan horses, worms and other forms of malware are a constant threat to computers of all kinds, cyber-criminals are turning to new techniques to infect and control your Mac. These new threats come silently, with little warning, over the Internet: in many cases, simply visiting a booby-trapped web page can compromise your Mac. Focusing on malware or network attacks alone is no longer sufficient to protect Macs from the dangers of the Internet. For this reason, Intego has decided to integrate the functions of its acclaimed VirusBarrier antivirus and NetBarrier personal firewall programs into a single application, optimized to manage the combined attacks that are increasingly common.

VirusBarrier X6, the latest version of Intego's network and malware security program, includes the many defenses that have protected Macs for more than ten years in earlier versions of VirusBarrier and NetBarrier, but adds much more. With multiple threat-detection techniques, improved methods of detection, combined detection protocols, proactive behavioral analysis, and a full range of defensive functions, VirusBarrier X6 protects Macs from all known network-based threats, as well as all known malware.

VirusBarrier X6 detects and eradicates:

- Mac viruses
- Windows viruses
- Unix viruses
- Microsoft Word and Excel macro viruses

- Trojan horses
- Worms
- Spyware
- Adware
- Hacking tools
- Dialers
- Keyloggers
- Rogue security programs, called "scareware"

Today's attacks include Trojan horses, cross-site scripting, spyware, clickjacking, phishing, poisoned JavaScript, malicious Java applets and much more. No longer do hackers create viruses just for the thrill of seeing computers getting infected. Cyber-criminals are in it for the money, and use their attacks to hijack infected Macs' DNS settings to send them to bogus web sites and harvest their passwords or credit card numbers. They create botnets, networks of infected computers, which respond to their controls to send out spam or attack other computers. They install rootkits to provide remote access to an infected computer, so they can steal passwords or other personal information. Or they create exploits that take advantage of vulnerabilities in Mac OS X, or in certain software it uses (Flash Player, QuickTime, PHP, Apache, etc.), to take over your Mac.

VirusBarrier X6 protects Macs from network intrusions by constantly filtering all the activity that enters and leaves through the Internet or a network. VirusBarrier X6 protects Macs from thieves, hackers and intruders, and warns users automatically if any suspicious activity occurs.

VirusBarrier X6 protects Macs from:

- Network intrusions
- Denial of service attacks
- Man-in-the-middle attacks
- Ping floods
- Port scans
- Cross-site scripting attacks
- Drive-by downloads
- Phishing
- Clickjacking
- Web pages with malicious JavaScript
- Malicious Java applets
- Rootkits

By combining the features of VirusBarrier and NetBarrier into a single program, Intego makes it easier for Mac users to protect themselves from all types of threats and attacks.

Installation

System Requirements

- Any officially-supported Mac OS X compatible computer
- Mac OS X 10.5 or higher; VirusBarrier X6 is fully compatible with Mac OS X 10.6 Snow Leopard and Mac OS X 10.5 Leopard. VirusBarrier X6 is not supported for use on Mac OS X Server.
- 100 MB free hard disk space

Installing Intego VirusBarrier X6

For information on installing and serializing Intego VirusBarrier X6, see the Intego Getting Started Manual.

Updating VirusBarrier X6 and Virus Definitions

Intego VirusBarrier X6 uses Intego NetUpdate, which is installed with the program, to provide updates to the program's filters and virus definitions, as well as to the program itself. For information on using NetUpdate, see the Intego Getting Started Manual.

About Your Copy of Intego VirusBarrier X6

To get information about your copy of VirusBarrier X6, choose **VirusBarrier X6** > **About VirusBarrier X6**. It gives information about Intego VirusBarrier X6, such as the version number, your support number (a number you will need for technical support), and a clickable link to send e-mail to Intego's support department.

Technical support

Technical support is available for registered purchasers of Intego products with valid subscriptions from the Intego Support page.

Getting Started with Intego VirusBarrier X6 ››

© 2011 Intego. All Rights Reserved.

Getting Started with Intego VirusBarrier X6

- Using the Setup Assistant
- Using the VirusBarrier X6 Overview Screen
- Status Indicators on the Overview Screen
- Malware Scanning at a Glance
- Using the Intego Menu

Go to Main Table of Contents

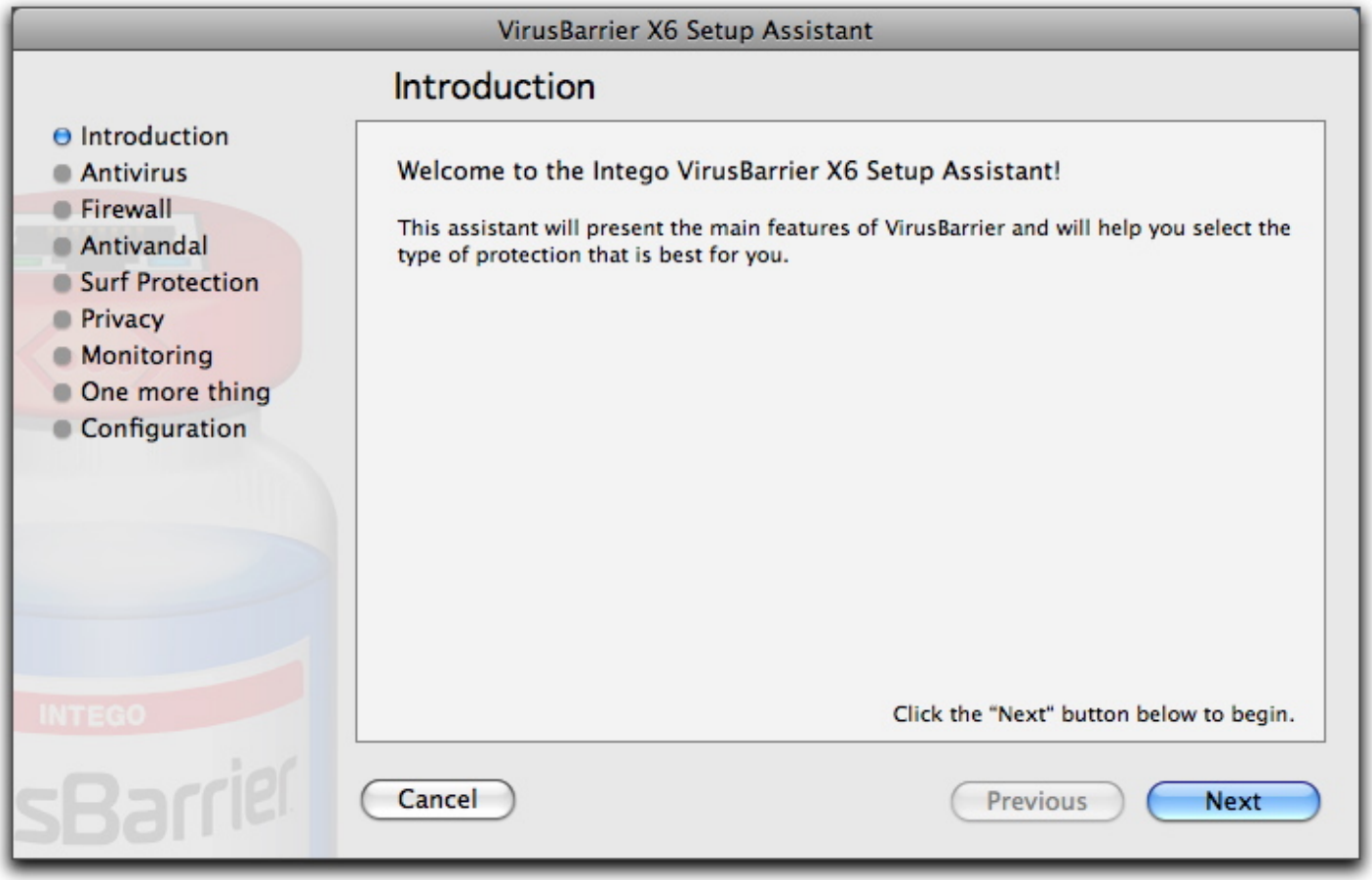
When you first launch VirusBarrier X6, you need to choose how to configure the program to provide optimal protection for the way you use your Mac. VirusBarrier X6 includes a Setup Assistant to help you do this, and to understand the many malware and network protection features the program provides.

Using the Setup Assistant

VirusBarrier X6's Setup Assistant helps you quickly and easily adjust the program's basic settings so they are appropriate to the way you use your Mac. The first time you open VirusBarrier X6, the Setup Assistant launches automatically.

If, at any time, you want to launch the Setup Assistant manually, you can do so by choosing **VirusBarrier X6** > **Preferences** and clicking the Advanced icon, then clicking **Show Assistant...**. You will need an administrator's password to run the Setup Assistant.

Note: if you have upgraded from a previous version of VirusBarrier or NetBarrier, the program will adopt the settings you had applied to those programs. If you had both of these programs, all settings will be imported; if you only had one of these programs, however, and you run the Setup Assistant, VirusBarrier X6 will overwrite your existing settings. In such cases, you may want to quit the Assistant and adjust malware or network protection settings manually.



The first eight screens of the VirusBarrier X6 Setup Assistant briefly present information about the program's various

functions:

- **Antivirus**
- **Firewall** (Rules and Trojans)
- **Antivandal** (Policy, Blocked Addresses and Trusted Addresses)
- **Surf Protection**
- **Privacy** (Anti-Spyware, Data)
- **Monitoring** (Monitoring tools)
- **One more thing** (miscellaneous tools)

When done, the Configuration screen allows you to choose which VirusBarrier X6 configuration you want to use.

The configurations are:

Name	This setting is best if...	Malware and Network Protection	Other settings
Basic	...you need to allow access to your Mac from the local network, but want to be protected from invasions from outside your local network.	The Real-Time scanner is active to protect you from malware. The firewall is set to "Client, local server" mode: your Mac can access the Internet as a client computer, and can function as both a client and server on a local network. Scanning for Windows and Linux malware is deactivated, and scanning for malware in archives is deactivated.	Antivandal filters are enabled against Buffer Overflow Attacks, Intrusion Attempts, Ping Attacks, Port Scans and SYN Flooding, but disabled against Ping Broadcasts. Anti-Phishing protection is enabled. Web Threat protection is disabled. Privacy filters are disabled.

Default	...you do not use your computer as a network server or for local file sharing.	The Real-Time scanner is active to protect you from malware. The firewall is set to "Client, local server" mode: your Mac can access the Internet as a client computer, and can function as both a client and server on a local network. Scanning for Windows and Linux malware is activated, as is scanning for malware in archives.	Antivandal filters are enabled against Buffer Overflow Attacks, Intrusion Attempts, Ping Attacks, Port Scans and SYN Flooding, but disabled against Ping Broadcasts. Anti-Phishing protection is enabled. Web Threat protection is enabled. Privacy filters are disabled.
Strong	...you want maximal protection, and can accept that this configuration might block some traffic.	The Real-Time scanner is active to protect you from malware. The firewall is set to Client only mode: your Mac can function only as a client on a local network or the Internet. The server functions of your computer are blocked.	All Antivandal filters are enabled, as are those that protect against Trojans. Anti-Phishing protection is enabled. Web Threat protection is enabled. Privacy filters are enabled.

After choosing your protection level, you have the option of running a full scan of your Mac immediately to ensure that it does not contain any malware, or to spot and eliminate any malware that is there. If you wish to do this, leave Perform a full scan after configuring checked. If you want to run this scan later, you can do so manually; in this case, uncheck this option. See later in this chapter for an introduction to scanning your Mac, and see Protecting Your Mac from Viruses and Malware for detailed information about running malware scans on your Mac.

Click the Configure button to activate the configuration you have selected and run a full scan of your Mac, if you have chosen to do this.

Using the VirusBarrier X6 Overview Screen

When you open VirusBarrier X6, the Overview screen displays. This screen displays information about how VirusBarrier X6 is running, and provides real-time feedback on its activities.

The Overview screen gives quick access to:

- VirusBarrier X6's functions, settings and logs,
- Several helpful network utilities, such as Whois and Traceroute,
- Visual indicators of what sorts of protection are enabled,
- Information about the program itself, such as when it was last updated,
- A way of managing multiple configurations, so you can quickly change protection settings.

At the top of the Overview screen is a row of buttons that provide access to VirusBarrier X6's many settings. The four leftmost buttons lead to settings that affect how VirusBarrier X6 protects you against malware. For details on these settings, see Protecting Your Mac from Viruses and Malware.

The four rightmost buttons lead to network protection controls. For details on these settings, see Protecting Your Mac from Network Attacks.

When you click buttons for malware or network protection, the resulting screens have tabs that lead to additional

controls. The Firewall button, for example, leads to a screen with two tabs, Firewall Rules and Trojan.

The center button in this row leads back to the Overview screen.

Any of these buttons glows green when the screen it leads to is active.

Controls for Monitoring are the smaller buttons in the bottom-right corner.

Monitoring functions are also available through selections under the View menu, and by using keyboard shortcuts. They are:

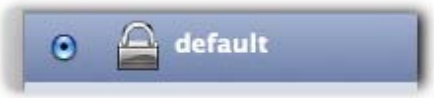
	Log	Option-Command-L	Shows a record of VirusBarrier's activities, and traffic to and from your Mac to the Internet or local networks
	Services	Option-Command-1	Shows a list of ways that your Mac is prepared to provide information to the outside world
	Traceroute	Option-Command-2	Shows the network path that a signal takes to get from your Mac to another computer
	Whois	Option-Command-3	Shows information about the owners and managers of Internet domains
	Traffic	Option-Command-4	Shows network traffic entering and leaving your Mac

	Networks	Option-Command-5	Shows outside networks that are currently available to your Mac

Each of these features is described in Using VirusBarrier X6 Monitoring Tools.

In the bottom-left corner is a button that reveals a list of Configurations. (You can also toggle between showing and hiding the Configurations list by pressing Command-K or choosing **View** > **Hide/Show Configurations List**.)

Each configuration is a collection of settings for VirusBarrier X6's malware and network protection. At first there is only one configuration, with either the name you chose in the Setup Assistant, or, if you did not run the Assistant, with the name "default". The radio button shows which configuration is currently active.

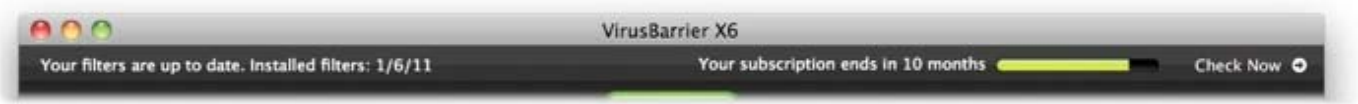


At the bottom of the Configurations list is an action button that lets you duplicate, edit and remove configurations. For more information, see VirusBarrier X6 Preferences and Configurations.

Next to the Configurations button is a Lock button, which allows you to lock VirusBarrier X6 so other users can't make changes to its settings. Since users who don't have administrator's accounts cannot make changes to VirusBarrier X6's settings, administrators will need to unlock the program to make changes. They can then click the Lock button to block access to settings again. (Non-administrators have access to all of VirusBarrier X6's scanning and monitoring features.)

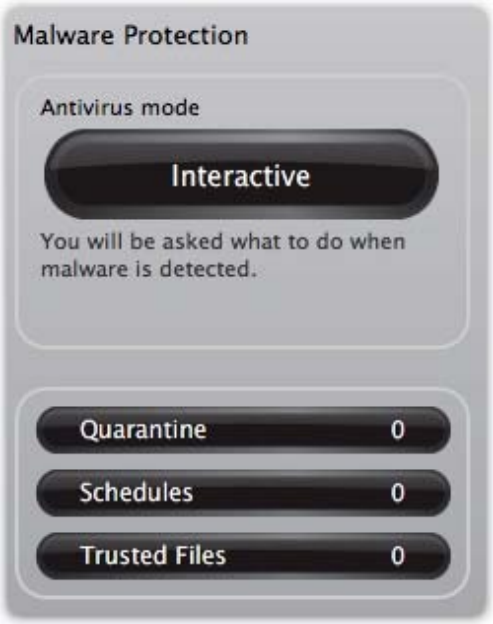
To lock VirusBarrier X6, either click the Lock button, press Command-L, or choose **File** > **Lock Settings**. To unlock VirusBarrier X6, click the Lock icon again, press Command-L or choose **File** > **Unlock settings**, then enter your administrator's password to complete the process.

At the very top of the screen is the NetUpdate Status Bar, which shows the dates of the latest VirusBarrier filters installed on your Mac, whether your filters need to be updated, and how much time remains on your subscription. VirusBarrier X6 uses Intego NetUpdate to periodically check for updates, or you can check manually by clicking Check Now in the upper-right corner. To hide the NetUpdate Status Bar, choose **File** > **Unlock settings**. For more on using NetUpdate, see the Intego Getting Started Manual.



Status Indicators on the Overview Screen

The status of various VirusBarrier X6 features appears on the Overview Screen. Indicators related to malware protection are on the left side of the screen.



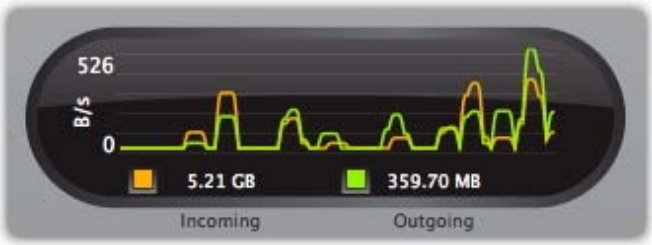
Indicators related to network protection are on the right side.

Clicking any of the indicators leads you to the screen where you can examine and change the settings relevant to that indicator.

The Anti-Phishing and Web Threat Protection indicators display green lights when enabled, as is shown above. When disabled, they display gray lights.

At the bottom left of the screen are two gauges that show current and past activity of the Real-Time Scanner, which continually monitors your Mac for malware infections.

The bottom-right part of the screen shows current network throughput, both incoming and outgoing.



Malware Scanning at a Glance

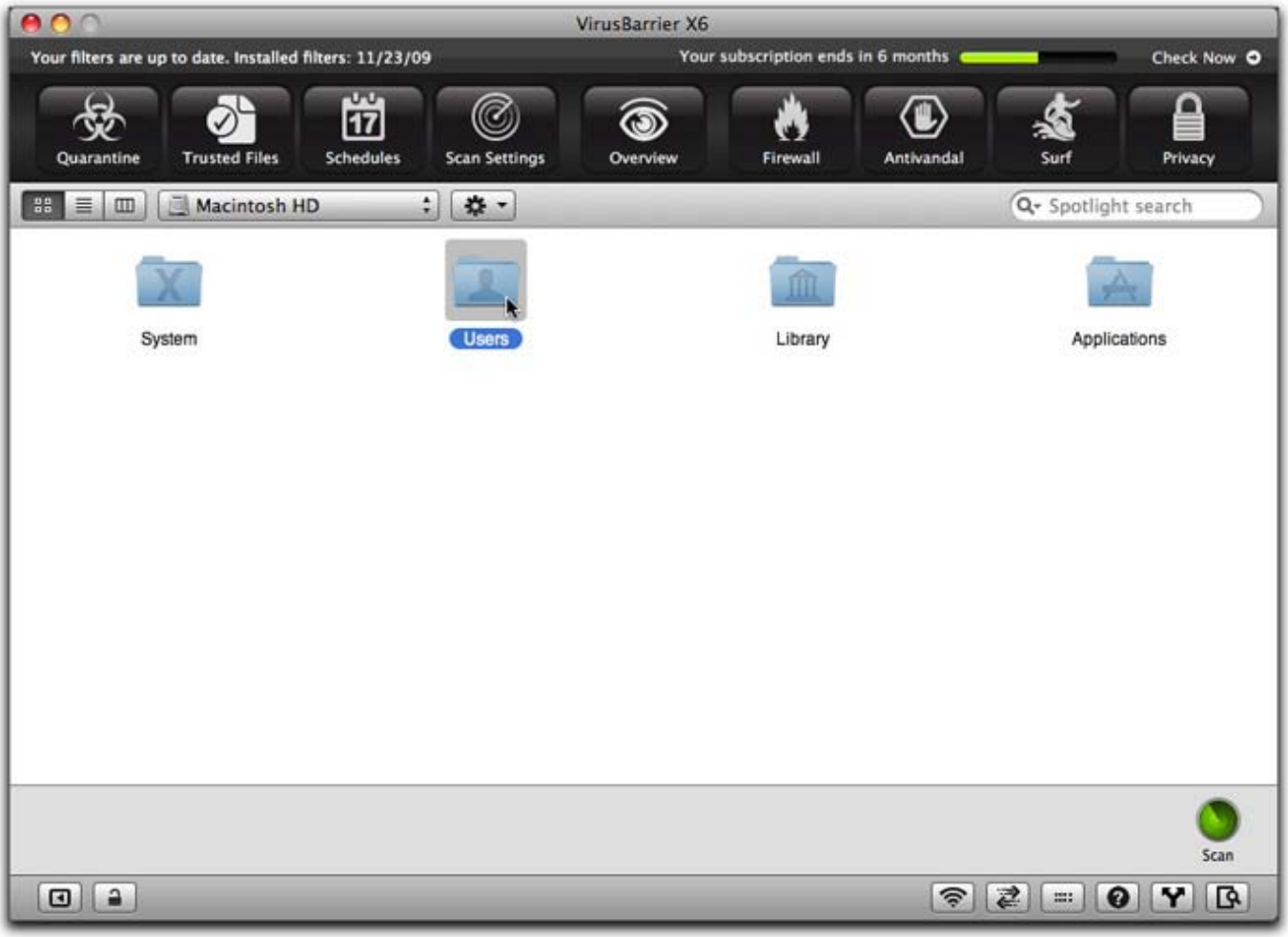
You can have VirusBarrier X6 automatically scan your Mac for malware after choosing your level of protection in the Setup Assistant, and VirusBarrier X6's Real-Time Scanner will then continue to monitor your computer to prevent possible infections. But you can also run a manual scan whenever you want. Full details are in Protecting Your Mac from Viruses and Malware, but here are a few tips to get you going quickly.

To scan your entire Mac, and any disks connected to it, just click the **Full Scan** button.

To quickly scan specific files or folders, simply drag and drop them either onto the program's icon in the Finder or in the Dock, or onto the Orb when VirusBarrier X6 is running.

To scan only selected files or volumes using the VirusBarrier X6 interface, click the **Select** button to see images of all the hard drives, volumes or other storage devices connected to your Mac.

Navigate to the file, folder or volume you want to scan in the same way you would in the Finder. Click to select the item, or press the Command key while clicking to select multiple items, then click the **Scan** button.

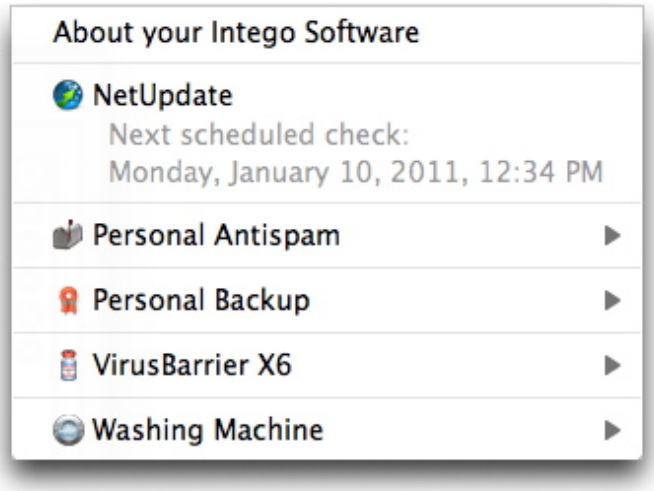


VirusBarrier X6 informs you if it finds files infected by any known malware. For more on VirusBarrier X6's alerts and what they mean, see Protecting Your Mac from Viruses and Malware.

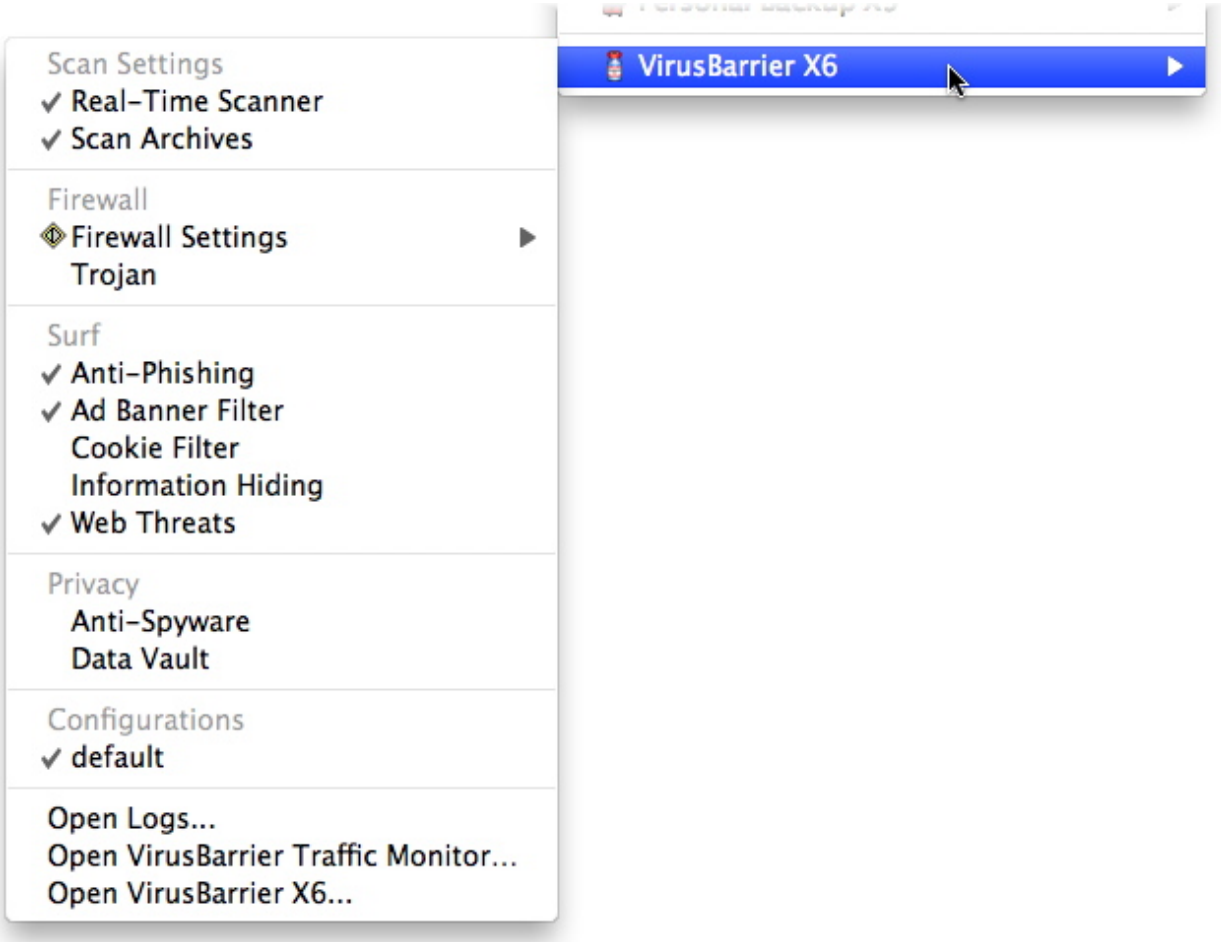
Using the Intego Menu

VirusBarrier X6 installs a menu in the menubar, called the Intego menu. Its icon is a small tower, as in the Intego logo.

Click the Intego menu icon to display a menu that shows all your Intego software:



You can change many of VirusBarrier X6's settings from the Intego menu. Choose the **Intego Menu** > **VirusBarrier X6**. You can start and stop the Real-Time scanner, you can change configurations, and you can turn settings on or off, such as Surf or Privacy settings. And you can open VirusBarrier Traffic Monitor by choosing its menu item near the bottom of the menu.



For more information about these features, see the appropriate sections of this manual: Protecting Your Mac from Viruses and Malware and Protecting Your Mac from Network Attacks.

‹‹ Welcome to VirusBarrier X6

Protecting Your Mac from Viruses and Malware ››

© 2011 Intego. All Rights Reserved.

Protecting Your Mac from Viruses and Malware

- Running Manual Scans
- Malware Alerts
- Scan Settings
- Trusted Files
- Quarantine Zone
- The VirusBarrier X6 Contextual Menu
- Using VirusBarrier X6 from the Command Line
- Using VirusBarrier X6 and AppleScript

Go to Main Table of Contents

VirusBarrier X6's anti-malware protection works in several ways. Its Real-Time Scanner constantly watches over your Mac, protecting you from viruses and malware. The Real-Time scanner ensures that your Mac is protected at all times by scanning every file that is created, copied, modified or saved. It does not, however, scan other files. This is why we suggest you run a full scan of all your files when you install VirusBarrier X6 and after each update to the program's virus definitions.

You can also use VirusBarrier X6's On-Demand scanner to check any file, folder, disk, or volume on your Mac.

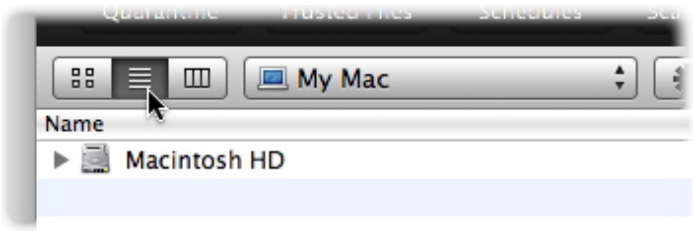
Running Manual Scans

You can run a manual scan with VirusBarrier X6 whenever you want. You should do this immediately after installation to ensure that you don't have any infected files; the VirusBarrier X6 Setup Assistant offers to do this after you first set up the program. After that, VirusBarrier X6's Real-Time scanner ensures that any new files you add to your Mac are safe.

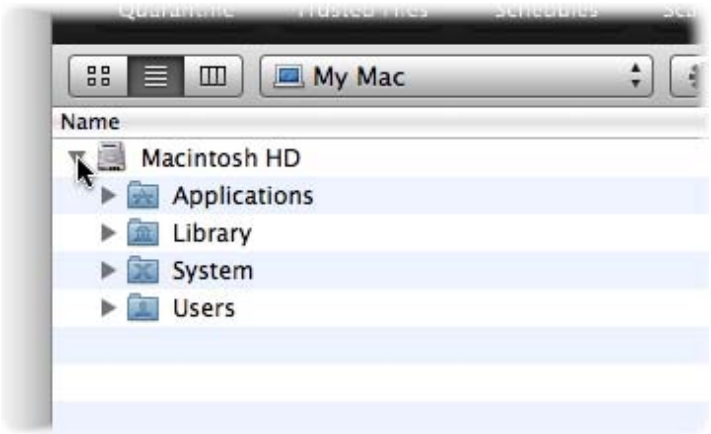
To quickly scan individual files or folders, simply drag and drop them either onto the program's icon in the Finder or in the Dock, or onto the Orb when VirusBarrier X6 is running.

You have additional scanning options when VirusBarrier X6 is running. First, click the **Select** button to see all the hard drives, volumes or other storage devices connected to your Mac. If you have an iPhone, iPad, iPod touch or AppleTV connected to your Mac, you will see these devices in the browser, and you can choose to scan them as well.

As in the Finder, you can see and select folders and files inside a volume by double-clicking it. You can also change the view to see your files as a simple list or in a file browser by clicking the view buttons in the window's upper-left corner.



In List view, you can display files inside a folder by clicking on its disclosure triangle, to the left of the folder's name.



Regardless of how you've chosen to view your files, you can select multiple items by holding down the Command key

as you click on each one in turn. When you've made your selection, click the Scan button in the bottom-right corner to begin the process.

By default, VirusBarrier X6 will first count the number of files to scan, then during the scan itself will display the number of files scanned and the percentage of the scan completed.

VirusBarrier X6 can scan files contained in compressed archives. When scanning archives, the Orb's display changes to show that it's working on an archive, and gives you an opportunity to skip the scanning of that archive, if it is very large and you are sure it is secure.

Note: When VirusBarrier X6 scans an iPhone, iPod touch, iPad or AppleTV, it scans files added by users, such as music, videos and photos. It also scans files added by third-party file transfer programs. If the device is jailbroken (unlocked using third-party software), VirusBarrier X6 scans all files on the device, including e-mails, personal files, and files added by third-party utilities.

When scanning an iPhone, iPod touch, iPad on AppleTV, VirusBarrier X6 copies all the files contained on the device to your startup volume in order to verify their security. If any malware or infected files are found, VirusBarrier X6 alerts you and offers to repair or delete the infected files.

You can stop a scan at any time by clicking the Stop button. If you wish to pause a scan, hold down the Option key on your keyboard and click this button, which now displays Pause.

To resume scanning, click this button, which now reads Resume.

When you run a manual scan, VirusBarrier X6 informs you if it finds files infected by malware. If any infected files are found, the VirusBarrier X6 Orb will turn red. If VirusBarrier X6 discovers any corrupted files, the Orb will turn orange. If both infected and corrupted files are found, the orb will blink red and orange. VirusBarrier X6 will also alert you according to the alert options you have set in the Preferences. For more on alert options, see VirusBarrier X6 Preferences and Configurations.

Quick Scans

VirusBarrier X6 lets you run quick scans, which scan only those locations where malware is commonly installed. The files and folders scanned may change as new malware appears, and the locations scanned may be different with newer versions of VirusBarrier X6's virus definitions.

To run a quick scan, click the Overview button on the VirusBarrier X6 window, if the Orb is not visible. Hold down the Option key, and you'll see that the **Full Scan** button changes to **Quick Scan**. Click this button to launch a quick scan.

Drag and Drop Scanning

You can scan any volume, folder or file by dragging it onto the Orb. You may need to enter an administrator's password if you do not have the appropriate permissions to access files contained in the item you drag onto the Orb.

You can also do this by dragging and dropping the volume, folder or file onto the VirusBarrier X6 program icon in the Finder.

Finally, you can drag and drop items to scan onto VirusBarrier X6's Dock icon.

Once you release the item to be scanned, Intego VirusBarrier X6 will start scanning it, the same as for any other manual scan.

Running Scans from the File Menu

You can launch scans from VirusBarrier X6's **File** menu. You can choose Scan (or press Command-O) to open the browser and select items to scan. You can also run a full scan by choosing Full Scan, or pressing Command-S, or a quick scan by choosing **Quick Scan** or pressing Command-Option-S. These scans run the same way as when you launch them manually, as described above.

Using the Mini Scanner

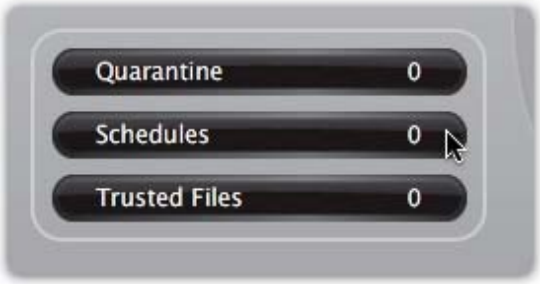
VirusBarrier X6 offers a small Mini Scanner window that you can use to run scans easily. To display this window, click the green button in the VirusBarrier X6 title bar, or choose **View** > **Switch to Mini Scanner**.

The Mini Scanner window floats above all other windows, so you can keep it in a corner of your screen and drag files onto the Orb at any time. To return to the normal view, click the green button, or choose **File** > **Switch from Mini Scanner**.

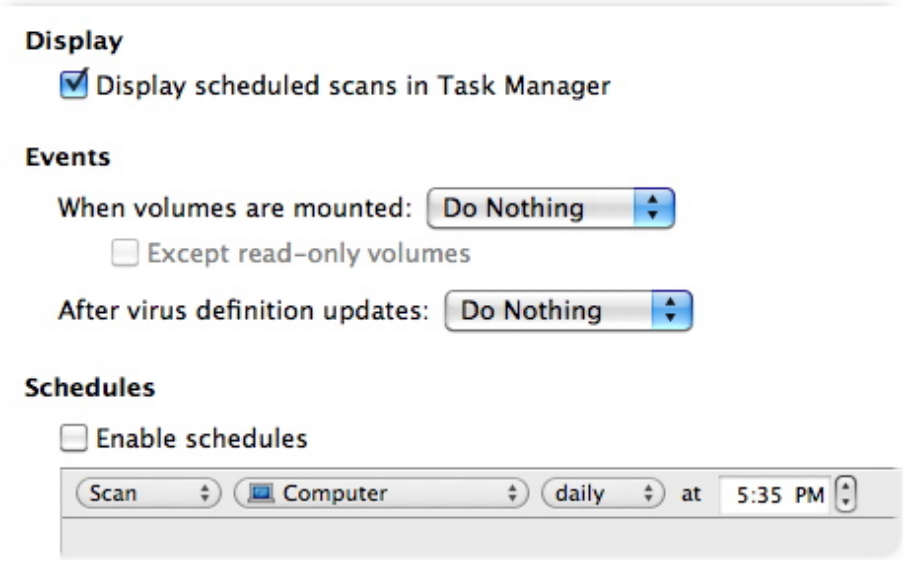
Scheduled Scanning

VirusBarrier X6 can also be set to run automatically at pre-arranged times. To do so, click the **Schedules** button at the top of the screen.

Or, when you're on VirusBarrier X6's Overview screen, click the **Schedules** button.



In either case, the Schedules window appears. There are three sections: Display, Events and Schedules



The **Display** section has only one checkbox: **Display automatic scans in Task Manager**. When checked, you'll see a small window appear whenever your Mac executes scheduled scans; when unchecked, such scans will occur without notification (unless malware is found).

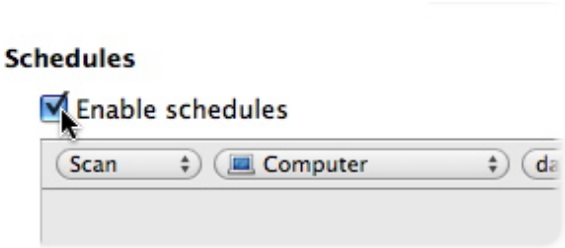
The **Events** section lets you direct VirusBarrier X6 to automatically run a scan, do repairs, or do nothing when certain events occur.

The first event, **When volumes are mounted:**, is triggered whenever you mount a new storage device, whether local (such as a hard drive) or remote (such as a network drive). If the **Except read-only volumes** checkbox is checked, VirusBarrier X6 will perform the action only on those volumes where it could change the drive being scanned (for example, to repair an infected file on a disk).

The second event, **After virus definition updates:**, lets you tell VirusBarrier X6 what to do after the program downloads and installs new virus definitions and filters. Virus definitions and filters are updated regularly, and especially when new malware is discovered to offer protection against that threat. Therefore, you should perform a new scan at those times to check for the new malware, either manually or (by checking this checkbox) automatically.

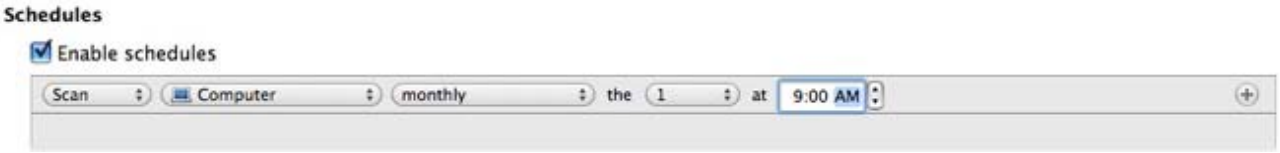
The **Schedule** section lets you determine when VirusBarrier X6 will run automated scans.

To turn on scheduling, click the Enable schedules checkbox.

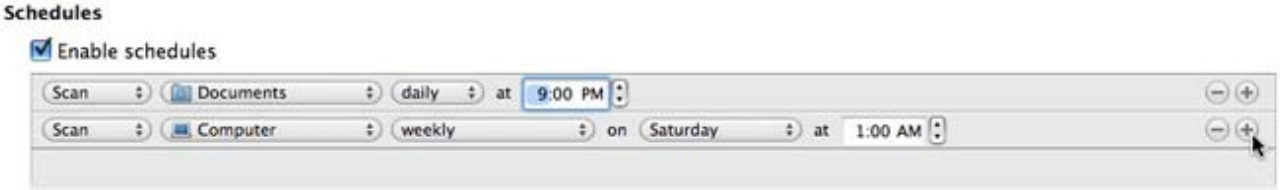


Below these settings is a scheduling selector, where you can say which folder should be examined, and when.

- The first popup menu lets you choose whether you'd like to **Scan**, **Quick Scan**, or **Repair** the selected files at the scheduled time. If you choose Quick Scan, you cannot choose specific folders to scan; the second menu will disappear.
- The second popup menu lists the folders you are most likely to want to scan, including your home folder and your Documents folder. The default choice, **Computer**, directs VirusBarrier X6 to scan all folders for all users on your Mac.
- The third popup menu lets you choose whether you want to perform the operation daily, weekly, or monthly. If you select **daily**, you'll be able to choose the time you prefer; select **weekly**, you'll also choose your preferred day; select **monthly**, and you'll choose which day of the month.



You can create multi-part schedules, for example to scan your Documents folder every night, and your entire computer once a week. To do so, click the + button to the right of the schedule item: another schedule item will appear beneath it. Make changes in that schedule item as you like. You can add as many schedule items as you like this way; to remove one of them, click the - button next to it.



The order of schedule items is not important; if you've scheduled two scans to run at the same time, they will occur simultaneously.

When you're done, the number of pending schedule items appears in the **Schedules** area on VirusBarrier X6's Overview window. To turn off all pending schedules, return to the Schedules and Events Preferences screen and uncheck the **Enable schedules** button.

Deactivating and Activating the Real-Time Scanner

There may be times when you want to deactivate VirusBarrier X6's Real-Time scanner. If, for example, you want to copy a large number of files from one disk to another, and you know the files are malware-free, turning off the Real-Time scanner may make your copy proceed a bit faster. To deactivate the Real-Time scanner, choose the Intego menu, which is in your menubar, then choose **VirusBarrier X6** > **Real-Time Scanner**; you'll see that this menu item becomes unchecked. To turn the Real-Time scanner on again, choose the same option in the Intego menu.

Malware Alerts

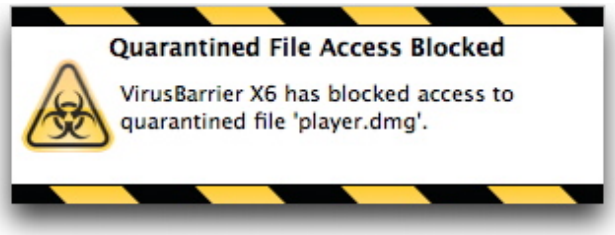
While VirusBarrier X6 can be used to run manual scans, as seen above, it is most effective when set to work in the background. VirusBarrier X6 has several ways of alerting you if it finds infected or corrupted files. This depends on how you scan the files, and what settings you have chosen in the Scan Settings pane for how the Real-Time scanner deals with infected files.

First, if you download an infected file from the Internet, or copy it from a hard disk or other storage device, and you have the Real-Time scanner active, and you have set it to ask what to do when infected files are found, VirusBarrier X6 will spot the malware and display an alert.

Depending on the type of alert, and the options you have set, you will have a number of choices. Clicking Reveal In Finder will show the file on your hard disk. If you want VirusBarrier X6 to repair the file, click Repair; to put it in the Quarantine Zone, click Put in Quarantine. (See the Quarantine section later in this chapter for more details.) If you don't want to do anything, click Ignore, and the file will not be repaired.

WARNING: Ignoring virus warnings can be dangerous! Only select to not repair files if you are sure of what you're doing.

If you have set VirusBarrier X6 to put infected files in the Quarantine Zone, or repair the files, a small alert displays.



If you scan items by dragging them on the VirusBarrier X6 Orb, the alert displays in a dialog in front of the VirusBarrier X6 window:

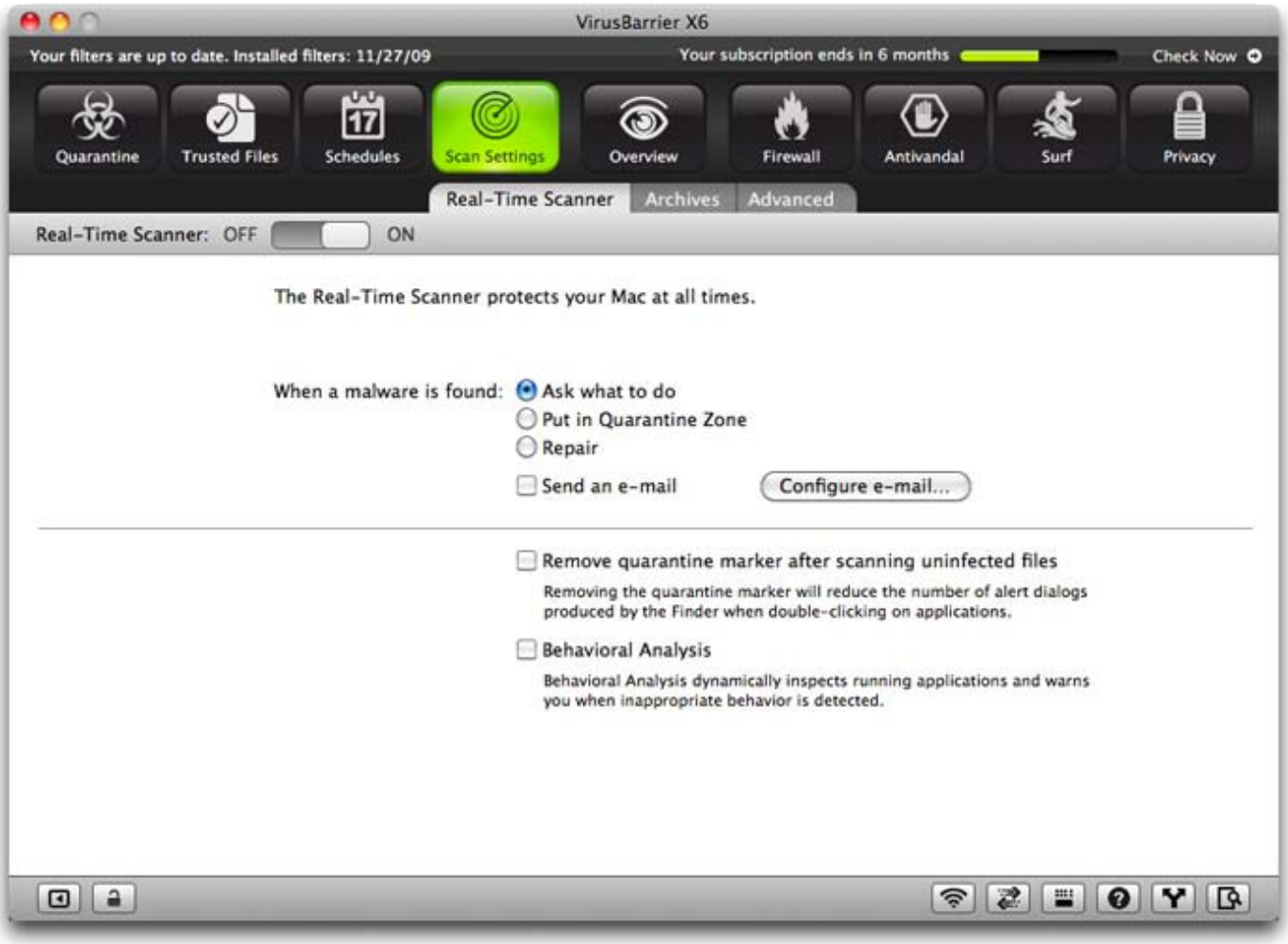
If you don't respond to a Real-Time scanner alert within one minute, VirusBarrier X6 places the file in the Quarantine Zone. (This doesn't apply to manual scans; when you scan files manually, the alert will remain displayed until you act.) You can check files that are in the Quarantine Zone later to decide what to do with them. See the Quarantine section later in this chapter.

For more on setting Alert preferences, see VirusBarrier X6 Preferences and Configurations.

Scan Settings

VirusBarrier X6 gives you a number of options that you can define to tell the program how it should scan your Mac, what types of files it should scan, and what types of malware it should look for. To access these settings, click the Scan Settings button.

The Scan Settings pane contains three tabs: Real-Time Scanner, which controls how VirusBarrier X6 runs scans in the background; Archives, which tells VirusBarrier X6 whether to scan archives and what types of archives to scan; and Advanced, which provides additional settings for both the Real-Time and On-Demand scanners.



Real-Time Scanner Settings

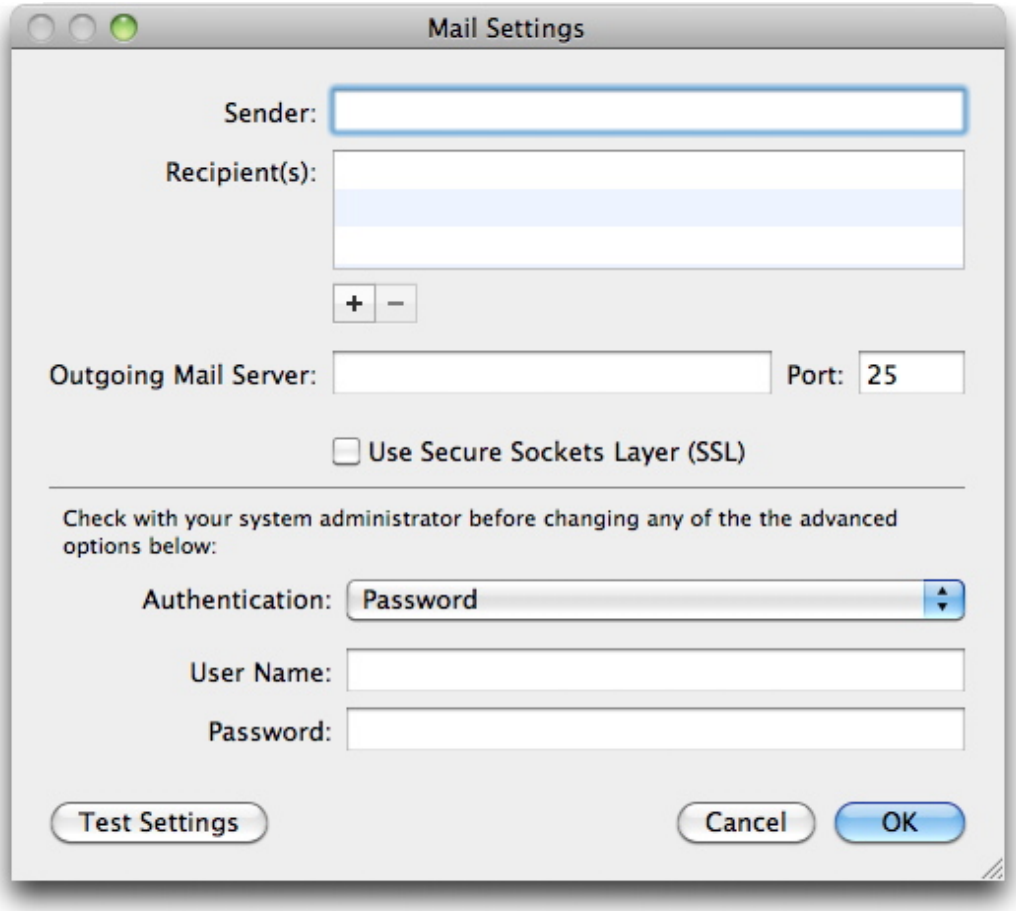
To turn off the Real-Time Scanner, move the Real-Time Scanner slider to **OFF**; you can turn it back on by moving the slider to **ON**. In normal operation, you will not need to disable the Real-Time Scanner; this is only useful for troubleshooting when you have a problem with your Mac. Note that you can also disable or enable the Real-Time Scanner from the Intego menu, by selecting **VirusBarrier X6** > **Real-Time Scanner**.

The next settings let you indicate what VirusBarrier X6 should do when it finds malware. Your options are:

- **Ask what to do**: this is most appropriate when you're running a virus scan on an "attended" Mac; that is, one that you're watching closely enough to see the alert when it pops up. Note that if you don't respond to an alert within one minute, VirusBarrier X6 places infected files in the Quarantine Zone.
- **Put in Quarantine Zone**: this ensures that the file cannot be opened or read. See the Quarantine Zone section below for more about using the Quarantine Zone.
- **Repair**: this tells VirusBarrier X6 to attempt to remove the malware. If, for any reason, the file cannot be

repaired, it will be placed in the Quarantine Zone.

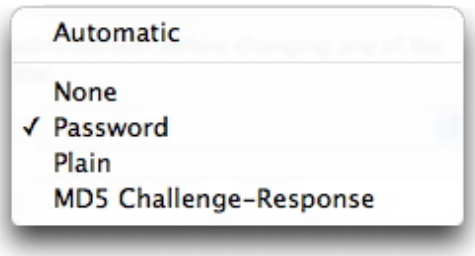
In addition, you can choose to have VirusBarrier X6 send you an e-mail whenever it discovers a virus. To set this up, check the **Send an e-mail** checkbox, then click the **Configure e-mail...** button next to it. The Mail Settings window displays.



You must enter e-mail addresses for the **Sender** and **Recipient(s)**, as well as the **Outgoing Mail Server**. Further, you'll need to enter a username and password that your mail server will accept. E-mail messages can be sent to multiple recipients. To add a recipient, click the + button. To remove a recipient, click the - button.

The lower half of the Mail Settings window deals with advanced options that VirusBarrier X6 may require to send e-mail.

The drop-down menu shows the various types of e-mail authentication handled, as shown below.

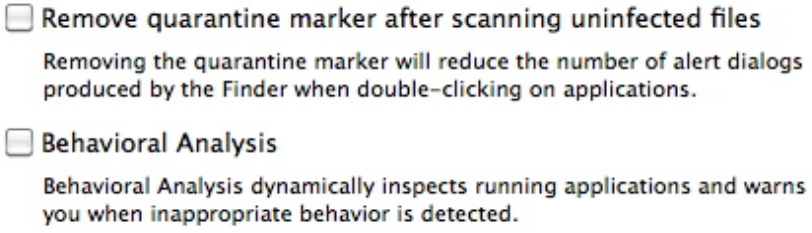


You should use the same **Authentication**, **User Name** and **Password** as you use in your usual e-mail program. If you're not sure what to enter here, check with your ISP or system administrator. If you don't know which type of authentication you use, select **Automatic**.

When you're done, you can confirm that the e-mail will go through by clicking the Test Settings button. You may have

to wait several seconds for your mail server to respond; when finished, a dialog box appears with the test's results.

The next section of the Real-Time Scanner settings window allows you to activate two settings.


Remove quarantine marker after scanning uninfected files
Removing the quarantine marker will reduce the number of alert dialogs produced by the Finder when double-clicking on applications.
Behavioral Analysis
Behavioral Analysis dynamically inspects running applications and warns you when inappropriate behavior is detected.

The first option, **Remove quarantine marker after scanning uninfected files**, tells VirusBarrier X6 to remove a quarantine marker set by Mac OS X when applications are downloaded and VirusBarrier X6 has found that they are not infected by any malware. This removes the Mac OS X dialog warning you that they were downloaded and asking if you're sure you want to open them.

The second option, **Behavioral Analysis**, tells VirusBarrier X6 to use Behavioral Analysis to keep an eye on suspicious activities performed by applications. If any application does anything that could be considered abnormal (such as deleting a large number of files, for example), VirusBarrier X6 will alert you to this.

Archive Settings

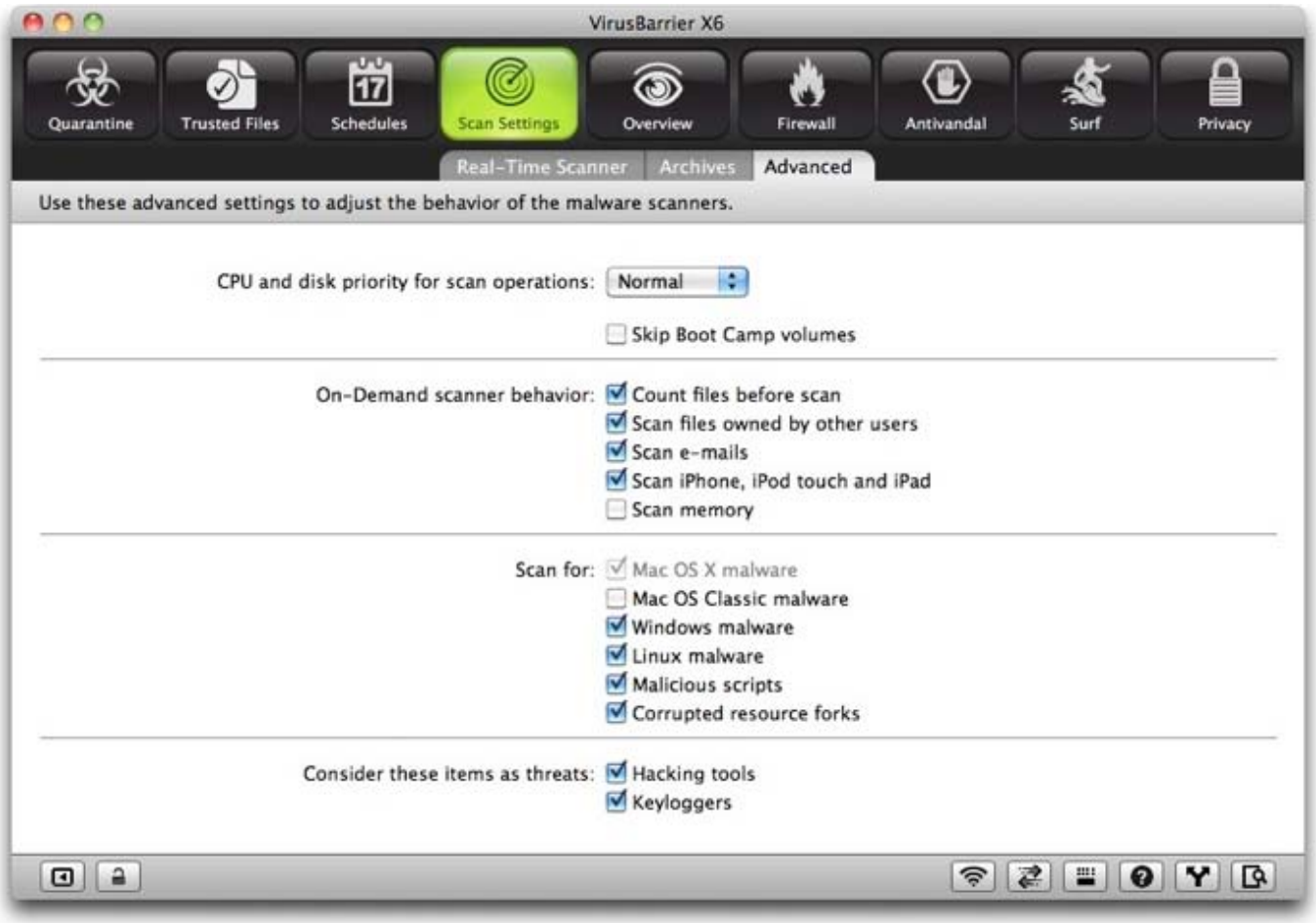
Archives contain one or more files, usually in a compressed format, so that they can be transferred easily and quickly. VirusBarrier X6 will look inside several popular types of archives, scanning not only the archive file itself, but also the files that it contains.

By default, VirusBarrier X6 will scan all archive types that it understands; however, you could choose to scan only certain archive types by unchecking different types of archives in the **Archive Kind** list. You can also, when running manual scans, skip any archives while they are being examined by clicking the **Skip** button in VirusBarrier X6's Orb. You may want to do this for large archives that take a long time to analyze, if you are sure they are free of malware.

The **Default archive timeout** setting lets you tell VirusBarrier X6 to stop scanning archives that take more than a certain amount of time to uncompress and scan. By default, this is set to 60 seconds. However, any files that have been uncompressed before the end of this timeout will be scanned.

Advanced Scan Settings

The Advanced tab provides a number of settings that apply to the On-Demand scanner, as well as some general scan settings.



The first available option is **CPU and disk priority for scan operations**. You can choose Low, Normal or High from a popup menu. This setting applies to manual scans and scheduled scans, and tells VirusBarrier X6 to adjust its scanning so other applications don't get slowed down. This setting affects both the processor (CPU) for the scan and the reading of your hard disk(s). Note that this also applies to scans set to run automatically when you mount external disks or after you update VirusBarrier X6's filters. So if you want those scans to complete more quickly, you should choose normal or high; if you don't care how long they take, or want your Mac to have more priority, choose Low.

The **Skip Boot Camp volumes** setting tells VirusBarrier X6 to not scan Boot Camp volumes during scans.

Five options affect On-Demand scanner behavior:

- The **Count files before scan** option makes VirusBarrier X6 count how many files are to be scanned, thereby

giving more accurate information on how long a scan is going to take by displaying a number of files and a percentage scanned in the Orb during a manual scan. With this option checked, VirusBarrier X6's Orb counts down as it scans, showing how many files remain to be checked; when it is not checked, the Orb counts up as it scans files, showing how many have been scanned.

- **Scan files owned by other users** allows VirusBarrier X6 to reach beyond the user account that's logged in at the time the scan begins to scan files on your Mac, including those belonging to other users. If you select this option, you'll immediately be required to enter an administrator password; if you don't have that password, the checkbox will revert to its unchecked state. If you don't check this option and VirusBarrier X6 finds an infected file owned by a different user or by the system, VirusBarrier X6's alert and Quarantine Zone window will display a crossed-out pencil icon, signifying that you will need to enter an administrator's user name and password to perform any action on the file.
- **Scan e-mails.** VirusBarrier X6 scans incoming and outgoing e-mails, both for their content and any attachments they contain, during manual scans.
- **Scan iPhone, iPod touch and iPad** tells VirusBarrier X6 to show any iPhone or iPod touch that is connected to your Mac when you run a manual scan so you can choose to scan the device for malware. If this option is unchecked, VirusBarrier X6 will not show any iPhone or iPod touch in its browser.
- **Scan memory** tells VirusBarrier to scan your Mac's active memory for traces of exploit code.

The **Scan for** section lets you choose to have VirusBarrier X6 scan files for specific types of malware:

- **Mac OS X malware**: this is dimmed, because it is always active. VirusBarrier X6 always scans for Mac OS X malware. This includes all types of malware that affects Mac OS X, such as Word and Excel macro viruses; the other categories are types of malware that cannot harm Mac OS X.
- **Mac OS Classic malware**: malware that only affects Classic Mac OS. If you still use any Mac OS Classic applications you can check this; if not, leave it unchecked.
- **Windows malware**: checking this tells VirusBarrier X6 to look for viruses that affect Windows. Although these files can't damage your Mac, you could pass them on to your Windows-using friends, and they could affect you if you use Windows on your Apple computer through a program such as Apple Boot Camp, VMware Fusion or Parallels Desktop. (VirusBarrier X6 does not, however, scan Windows virtual disks.)
- **Linux malware**: if this is checked, VirusBarrier X6 will scan for malware that affects the Linux operating system.
- **Malicious scripts**: checking this tells VirusBarrier X6 to scan for malicious scripts such as PHP, shell scripts, JavaScripts, Perl, etc.
- **Corrupted resource forks**: while this type of corrupted file is not necessarily malware, corrupted resource forks – parts of certain files – can cause Macs to crash in certain cases. Checking this can protect your Mac from crashes caused by this type of corrupted file.

A final section lets you choose to look for two other types of malware:

- **Hacker tools** are malicious programs that may not directly harm your Mac, but that may be used by hackers to attack other computers. It is especially useful to check this option if your Mac is publicly accessible.
- **Keyloggers** are programs that record all your keystrokes. While some such programs may be malicious, others may be installed intentionally to monitor computer users, such as children. If this is checked, users being monitored may be alerted to the existence of such software on their Mac.

Trusted Files

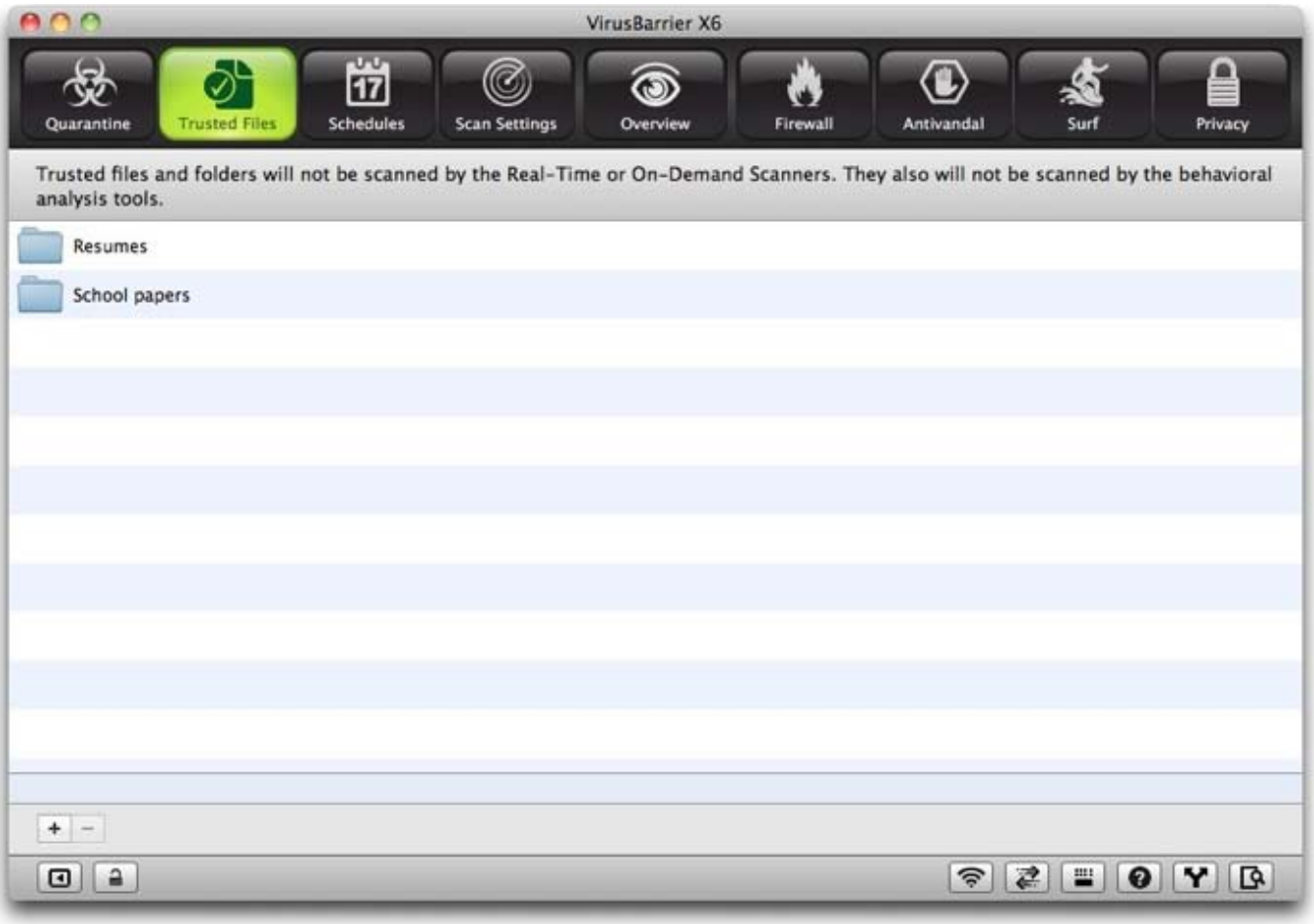
VirusBarrier X6 offers the option to add files, folders or volumes to a list of Trusted Files. VirusBarrier X6 will assume that these files are all safe and will not scan them. You should only use this for files that have already been scanned by VirusBarrier X6.

There are two ways to add files, folders and volumes to the Trusted Files list. First click the **Trusted Files** button:

Then, do one of the following:

- Click the small + button at the bottom-left corner of the screen, navigate to the item you'd like to add to the Trusted Files list, then click the **Add** button, or
- Drag the item from the Finder into the window

Adding a folder or volume tells VirusBarrier X6 to trust *all* files contained in the selected item, including in any subfolders it contains.



To remove an item from the Trusted Zone, click it to select it, then click the - button.

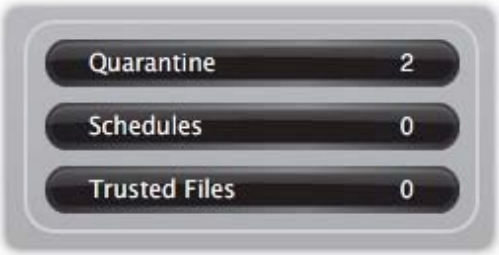
You can also use the Contextual Menu to add items to the Trusted Zone: See this chapter's section about the Contextual Menu, below, for more information.

Quarantine Zone

If you don't want to repair files automatically, you can have VirusBarrier X6 put them in its Quarantine Zone. When files are quarantined, they can't be opened or read, ensuring that they cannot infect your Mac. This is useful for

administrators who want to check files before running VirusBarrier X6's repair functions.

As mentioned above when discussing alerts, VirusBarrier X6 automatically places files in the Quarantine Zone if you don't respond to an alert within one minute. You can then check these files and decide what to do. The Quarantine button on VirusBarrier X6's Overview screen shows you which files are quarantined.



To see which files are quarantined, either click that button, or click the **Quarantine** button at the top of the screen.

You'll see a display that shows which files are in the Quarantine Zone, as well as a group of buttons allowing you to act on those files.

You can view quarantined files either as Icons or List items by clicking one of the view buttons at the top left of the window.

To act on any of the files, select them and then click one of the four buttons at the bottom right of the window.

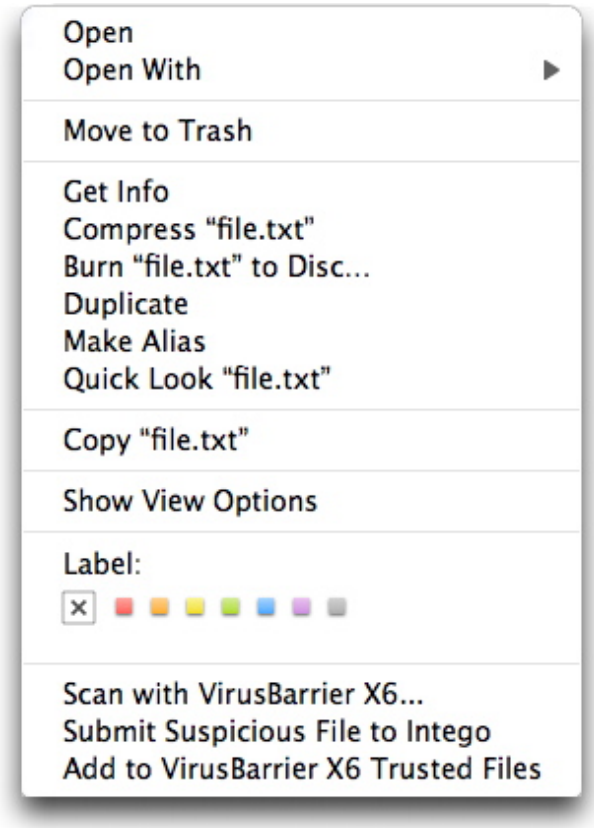
You can do the following:

- **Delete from Disk** removes the file from your Mac.
- **Consider Safe** tells VirusBarrier X6 that you think this file is not infected, and adds the file to VirusBarrier X6's Trusted Files list. This may occur for false positives. However, be *very careful* when you click this button: only do so if you are sure the file is safe. If not, it may infect your entire Mac.
- **Scan** tells VirusBarrier X6 to scan the file again. You may want to do this after updating virus definitions to ensure that the file wasn't flagged incorrectly as a false positive.
- **Repair** tells VirusBarrier X6 to remove the malware from the file.

If you display the Quarantine Zone in list mode, a Threat column will tell you which types of malware your files are infected by.

The VirusBarrier X6 Contextual Menu

You have access to a number of VirusBarrier X6's features directly from the Finder using a Contextual Menu. Control-click or right-click on any item – a file, folder or volume – and a contextual menu will open. In Mac OS X 10.6, Snow Leopard, these menu items are grouped at the bottom of the contextual menu; however, if you have enough such items, you'll find a **Services** menu item, and VirusBarrier X6's menu items will be in the **Services** sub-menu. In Mac OS X 10.5, Leopard, the VirusBarrier X6 menu appears under a "More" menu.



The contextual menu lets you do the following:

- Scan the selected item (and repair it if your settings allow).
- Send a copy of the item to Intego by selecting **Submit Suspicious File to Intego**. This is especially useful if you have files that you suspect are infected with new or unrecognized viruses. If you choose this option, Intego's

virus experts can examine the file and produce the virus definitions you and other users will need to protect their systems, if necessary.

- Add the item to the Trusted Files list.

Using VirusBarrier X6 from the Command Line

VirusBarrier X6 also gives you the option of running malware scans and changing settings to network protection from the command line. The following describes the use of this command.

```
Command:

/Library/Intego/virusbarrier.bundle/Contents/MacOS/virusbarriers [-rtcCaz]
<pathname_to_scan> [<current_directory_pathname>]

The following options are available:

-a:    Scans all files, including those symlinked to other volumes
       (or other mount points in /Volumes).
-c:    Counts files before scanning.
-C:    Counts files, but does not scan.
-Q:    Performs a quick scan.
-r:    Repairs infected files.
-t:    Uses Turbo Mode; scans only those files that have not been modified
       since the previous scan.
-T:    Scans all but trusted files.
-z:    Scans compressed archives (including those in e-mail attachments).

<pathname_to_scan>: This is required; it can be a relative or absolute path.

[<current_directory_pathname>]: This is optional; it is the current working
directory if a relative path is used as the first argument.

Example:

/Library/Intego/virusbarrier.bundle/Contents/MacOS/virusbarriers -tacz /

This scans all volumes for which the user has read permission, scanning archives
and counting the number of files to scan before beginning. If you run the
command preceded by sudo, and authenticate, you can scan all files.

You can also define aliases to simplify the use of this command.

For bash:

alias vbscan=/Library/Intego/virusbarrier.bundle/Contents/MacOS/virusbarriers

For tcsh:

alias vbscan /Library/Intego/virusbarrier.bundle/Contents/MacOS/virusbarriers

This allows you to run the same command as follows:

vbscan -tacz / [-rtcCaz] <pathname_to_scan> [<current_directory_pathname>]

To change network protection settings, use the following option, along with the
operations, objects and data listed below (all commands with firewall options
require sudo):

-W: Execute firewall operations

operation          object                                data
-------------------------------------------------------------------
import|export      settings                              file_path
revert             settings
add|remove         blocked_address|trusted_address       ip_address
print              blocked_address|trusted_address
get                protection
enable/disable     protection
enable/disable     trojans
enable/disable     data
enable/disable     antispyware
enable/disable     banner_filter
enable/disable     cookie_filter
enable/disable     information_filter
enable/disable     webthreats
enable/disable     antiphishing
activate           configuration                         configuration_name
print              configuration
reset              traffic
reset              cookie

For example, to enable firewall protection, run the following command with sudo:

/Library/Intego/virusbarrier.bundle/Contents/MacOS/virusbarriers -W enable protection
```

Using VirusBarrier X6 and AppleScript

VirusBarrier X6 offers the ability to run scans using AppleScript. For more information on the program's AppleScript syntax, open the VirusBarrier X6 dictionary from AppleScript Editor.

‹‹ Getting Started with Intego VirusBarrier X6

Protecting Your Mac from Network Attacks ››

© 2011 Intego. All Rights Reserved.

Protecting Your Mac from Network Attacks

- Using the VirusBarrier X6 Overview Screen
- Status Indicators on the Overview Screen
- Firewall Protection
- Trojan Horse Protection
- Antivandal Protection
- Blocked Addresses and Trusted Addresses
- Surf Filters
- Privacy Protection
- Understanding Alerts

Go to Main Table of Contents

In addition to its powerful anti-malware features, VirusBarrier X6 protects your Mac from network attacks and web threats using a number of powerful features. These features can be broken down into four groups:

- **Firewall**, which defines the network communications that your Mac will allow;
- **Antivandal** tools, which monitor communications for several types of network attacks;
- **Surf** tools, which watch for "social engineering" attacks based on your online behavior, and protect against web threats; and
- **Privacy** protectors, which let you decide which programs can connect to a network, and which data they're forbidden from sending.

These four defenses protect you against virtually every kind of attack possible, including Trojan horses, ping attacks, and port scans. Together with its malware protection, VirusBarrier X6 offers total network and malware protection for your Mac.

Launching VirusBarrier X6 brings you to the Overview screen, which you can always return to by clicking the **Overview** button in the middle of the top row of buttons. The screen is divided into columns: to the left of the central Orb are Malware Protection tools, and to the right are the Network Protection tools we'll discuss in this chapter. Malware protection is discussed in Protecting Your Mac from Viruses and Malware.

Using the VirusBarrier X6 Overview Screen

The Overview screen gives quick access to:

- Virus protection tools, which are discussed in Protecting Your Mac from Viruses and Malware;
- VirusBarrier X6's functions, settings and logs;
- Several helpful network utilities, such as Whois and Traceroute;
- Visual indicators of what sorts of protection are enabled;
- Information about the program itself, such as when it was last updated;
- A way of managing multiple configurations, so you can quickly change protection settings.

Central to the Overview screen are sections that control VirusBarrier X6's four lines of network defense. Controls for **Firewall**, **Antivandal**, **Surf** and **Privacy** protection appear as large buttons at the top right of the Overview screen; they are green when selected and black when unselected. Controls for monitoring are the smaller buttons in the bottom-right corner. In between those two groups are helpful indicators that lead you to relevant controls when clicked.

	The Firewall section gives you access to rules that define which programs can send and receive information to and from your Mac.
	The Antivandal section gives you ways to stop certain types of network attacks and choose policies to determine how to handle attacks when they occur.

	The Surf section blocks certain types of information from being sent and received when you surf the Internet, protecting you from phishing attempts, ads, and cookies. It also lets you hide certain information your browser customarily transmits.
	The Privacy section gives you access to settings that prevent specific data from being sent over the Internet and local networks, and its Anti-Spyware tools protect you against programs that secretly connect to remote computers.

You can access Monitoring functions through buttons in the bottom-right corner of the Overview screen. See Using VirusBarrier X6 Monitoring Tools for more on using these features.

VirusBarrier X6 lets you create different configurations, which are groups of settings for the program's various features. To see a list of configurations, click the small arrow button in the bottom-left corner of the Overview screen. (You can also toggle between showing and hiding the Configurations list by pressing Command-K or choosing **View** > **Hide/Show Configurations**.)

At first there is only one configuration, named according to the settings you chose in the Setup Assistant, when first launching the program, or "default" if you did not run the Setup Assistant. The radio button shows which configuration is currently active.

At the bottom of the Configurations list is an action button that let you duplicate, edit and remove configurations. For more information, see VirusBarrier X6 Preferences and Configurations.

At the very top of the screen is the NetUpdate Status Bar, which shows the dates of the latest VirusBarrier filters installed on your Mac, and the date of the latest filters available. VirusBarrier X6 uses Intego NetUpdate, installed with the program, to update filters and virus definitions as well as Intego programs themselves. It checks for updates automatically, and you can have it check immediately by clicking the **Check Now...** button in the upper-right corner. To hide the NetUpdate Status Bar, choose **View** > **Hide NetUpdate Status Bar**. For more on using NetUpdate, see the Intego Getting Started Manual.

Status Indicators on the Overview Screen

The status of various VirusBarrier X6's network protection features appears as a stack of clickable indicators in the right column of the Overview screen.

The top indicator tells you which **Firewall** mode you've selected; clicking it leads you to a screen where you can change that setting. (The large **Firewall** button at the top of the screen leads to the same place.)

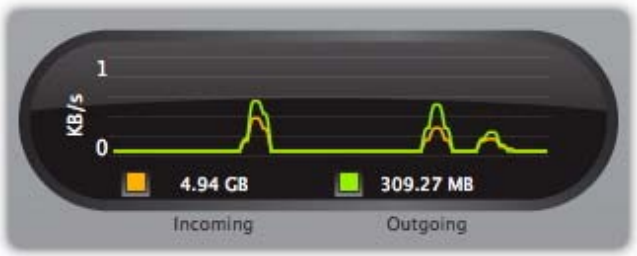
Network Protection
Firewall mode
Client, local server
Only computers on your local network can connect to your Mac as a server. You still have access to the Internet.

The first indicator of the middle group tells you whether **Anti-Phishing** protection is enabled. "Phishing" is a kind of attack where a cyber-criminal attempts to trick you into entering private information, such as financial data or a password, in order to gain access to personal data, such as that for e-mail accounts or even bank accounts. Clicking this button leads you to a screen where you can add sites that you trust, and should therefore be exempted from Anti-Phishing protection. (You can also reach this screen by clicking the large **Surf** button at the top of the screen, and then clicking the **Anti-Phishing** tab.)

The second indicator in that group tells you whether **Web Threat Protection** is enabled. Clicking this button leads you to a screen where you can add sites that you trust, and should therefore be exempted from Web Threat protection. (You can also reach this screen by clicking the large **Surf** button at the top of the screen, and then clicking the **Web Threats** tab.)

The bottom indicator in this group shows the number of addresses that have been blocked, that is, forbidden to communicate with your computer. These addresses are blocked either because VirusBarrier X6 found them to be malicious, or because you added them manually. Clicking this button leads you to a screen that shows you which addresses are blocked, and details about why they were blocked and how long they will continue to be blocked. (You can also reach this screen by clicking the large **Antivandal** button at the top of the screen, and then clicking the **Blocked Addresses** tab.)

The last indicator in the Network Protection column is the Network Traffic indicator, which updates in real time to show how much data is entering and leaving your computer. This indicator is not a button, so clicking it does nothing; for more details on your network traffic, click the Traffic monitoring button in the bottom-right corner of the screen.



Firewall Protection

VirusBarrier X6 includes a personal firewall, a powerful feature that filters all data packets entering or leaving your Mac through the Internet or a local TCP/IP network. It also protects you from Trojan horses by blocking the ports they use.

To view or change Firewall settings, click the **Firewall** button.

When you click the Firewall button, VirusBarrier X6 presents its Simple mode for controlling Firewall settings. There are five preset firewall settings that cover all the situations that you will encounter in normal use, each accompanied by an animation that graphically shows the effect of applying the setting. The screen closest to you represents your Mac; the globe represents the Internet; the screen halfway between the two represents the limit of your local network. Here the default setting, "Client, local server", shows how your computer can receive information from beyond the local network, but that computers beyond your local network cannot access your Mac.

The five standard firewall settings are:

- **No restrictions**: VirusBarrier X6's firewall allows all incoming and outgoing network data to be sent and received.
- **No network**: VirusBarrier X6's firewall prevents all data from entering or leaving your computer to or from the Internet or a local TCP/IP network. This is useful if you are away from your computer and wish to protect it totally.

- **Client, local server**: VirusBarrier X6's firewall allows your Mac to function as a client and local network server. Your Mac can access the Internet as a client computer, and as both a client and server on a local network.
- **Server only**: VirusBarrier X6's firewall allows your Mac to function only as a server: all client functions, including your ability to surf the Internet, are blocked.
- **Client only**: VirusBarrier X6's firewall allows your Mac to function only as a client on a local network or the Internet. The server and file-sharing functions of your Mac are blocked.

These five settings are sufficient for most people. But if you want more control over access to your computer – if, for example, you're running a gaming party and want to forbid all traffic except for communications that are part of the game – then you need to switch to VirusBarrier X6's Advanced mode.

Advanced Mode

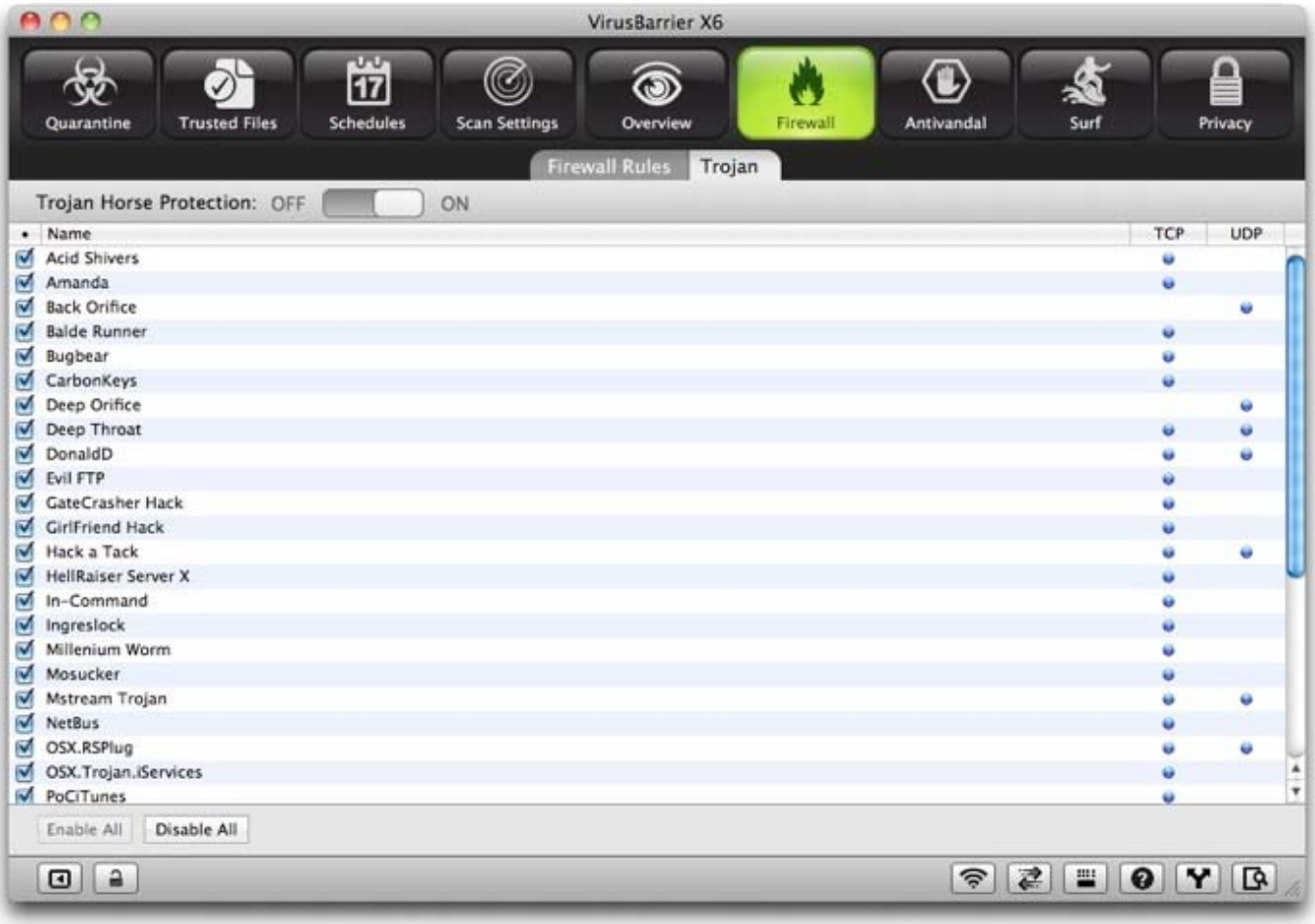
VirusBarrier X6 also offers an advanced firewall mode you can use to create your own rules to choose exactly which types of traffic you want to allow or block to and from your Mac. For more on using Advanced Mode, see Appendix: Creating Custom Firewall Rules.

Trojan Horse Protection

Trojan horses are applications that are surreptitiously installed on your computer, either by attachments you receive with e-mail messages, or by programs you download from malicious web sites. In some cases, programs install a specific type of Trojan horse, known as spyware, which sends your personal information to a server. Since the connection is made *from* your computer, it is generally trusted.

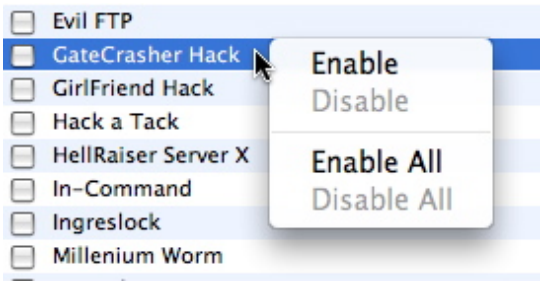
VirusBarrier X6 knows how to spot the actions of the most common Trojan horses and stop them in their tracks. Some such programs send information about users' browsing habits to a central server; other Trojan horses open "back doors" in your computer that allow hackers to take control of it or steal files. In addition, VirusBarrier X6 recognizes the actions of Windows Trojan horses, so if you are running Windows in virtualization – with a program such as VMware Fusion or Parallels Desktop – and sharing your Mac's Internet connection in NAT mode, you'll be protected.

To see VirusBarrier X6's Trojan Horse controls, click the **Trojan** tab at the top of the Firewall screen.



To turn on Trojan horse protection, set the **Trojan Horse Protection** slider to **On**, then click the checkboxes of individual Trojans to select them. The **Enable All** and **Disable All** buttons at the bottom are handy shortcuts that select or deselect all checkboxes at once.

You can also enable Trojan blocking for an individual Trojan horse, or for all Trojan horses, by holding down the Control key on your keyboard and clicking on the name of a Trojan, and choosing the appropriate command from the contextual menu that displays.

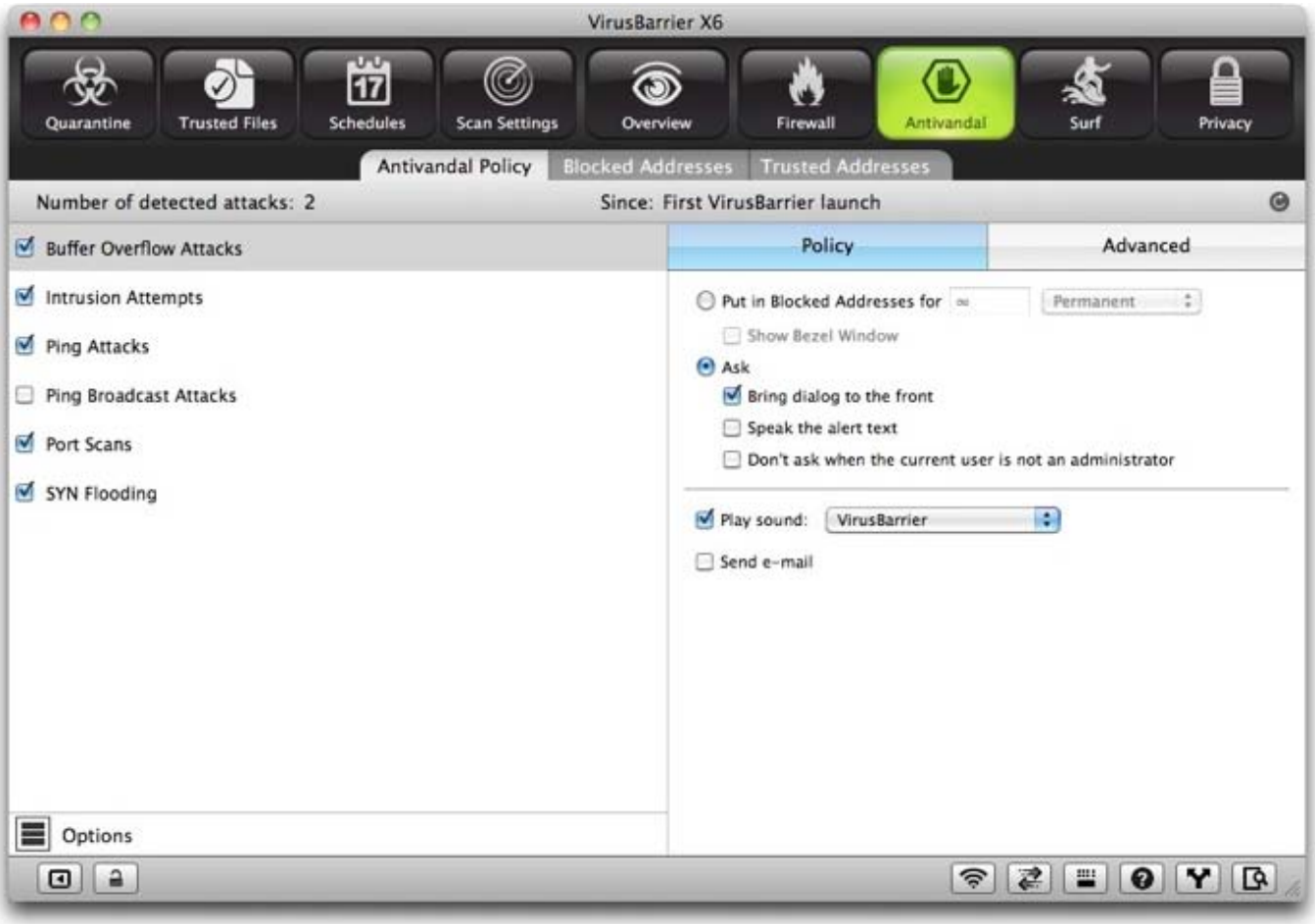


Antivandal Protection

VirusBarrier X6's Antivandal watches over data entering your Mac and filters it, looking for signs of intrusion. This filtering is transparent: the only time you'll see signs of it working is if it detects suspicious data, in which case an alert displays. Otherwise, Antivandal silently monitors your Mac's network activity at all times.

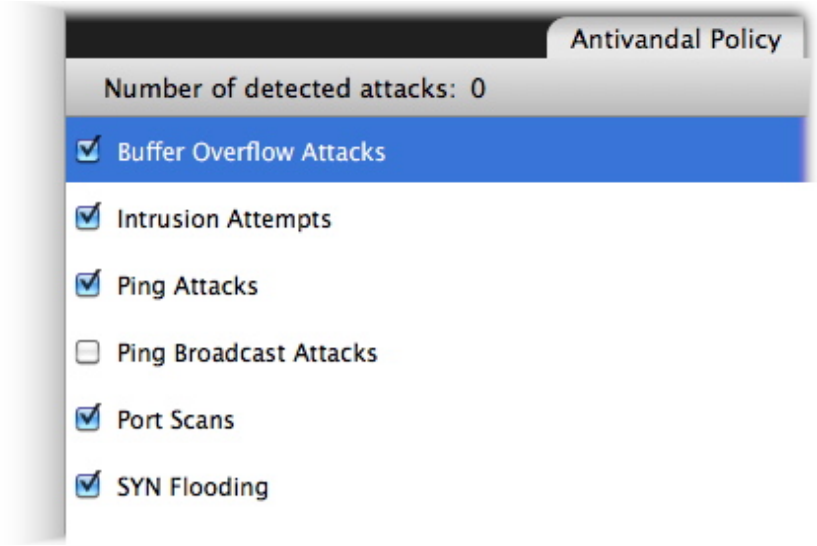
To go to the Antivandal screen, click the **Antivandal** button.

The Antivandal Policy tab controls how data entering your computer is filtered. The **Blocked Addresses** and **Trusted Addresses** tabs store specific hosts, or IP addresses, that you deem suspicious or trustworthy.



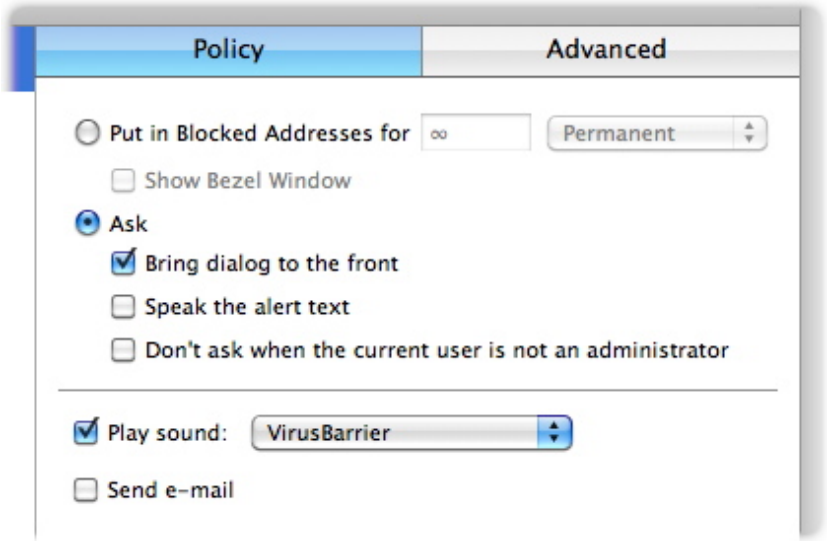
Antivandal Policy

The **Antivandal Policy** panel provides tools to prevent six types of intrusions.



- **Buffer Overflow Attacks**: Attacks that may occur when certain software has flaws in the way it handles memory, allowing malicious users to get into your Mac.
- **Intrusion Attempts**: Attempts to access your Mac through a preset number of incorrect password requests within a given period of time. Different settings are available for AppleShare IP (ASIP), FTP, HTTP, IMAP, POP and SMTP.
- **Ping Attacks**: Your Mac receives a number or frequency of ping requests so great that responding would cause a strain on your Mac.
- **Ping Broadcast Attacks**: Ping requests to broadcast addresses, where a single ping is multiplied throughout your local network.
- **Port Scans**: Attempts by remote computers to search your Mac's ports for vulnerabilities. You may want to leave this unchecked if your computer is functioning as a server.
- **SYN Flooding**: Multiple TCP requests sent by an attacker who then doesn't complete the final stage of the exchange, causing the target computer to consume resources.

Clicking the checkbox next to each of these enables or disables protection for that intrusion type. Clicking on the name of the intrusion type shows the notification and action policies for that intrusion type. Here, for example, we see the policy for Buffer Overflow Attacks.



These options are described later in this chapter, in Understanding Alerts.

While an intrusion type is selected, clicking the Advanced tab in the right-side pane brings up additional options that

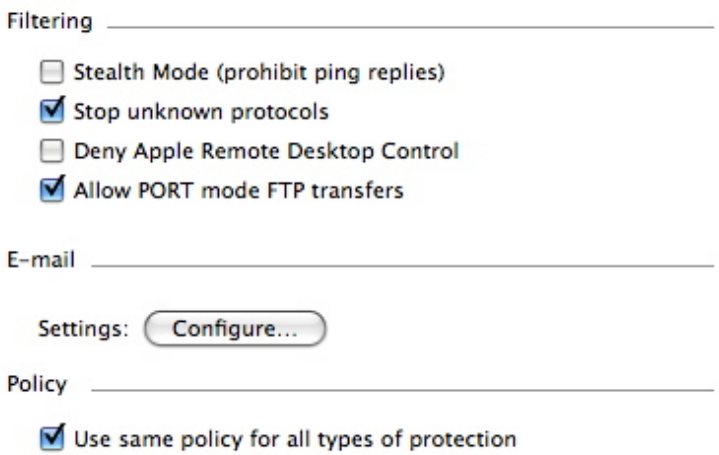
are specific to that intrusion type. These are:

- **Buffer Overflow Attacks**: No advanced settings.
- **Intrusion Attempts**: You can separately set the number of incorrect password attempts permitted for AppleShare IP (ASIP), FTP, HTTP, IMAP, POP and SMTP.
- **Ping Attacks**: Ping flood sensitivity, measured in milliseconds (ms) permitted between ping attempts. If your computer is on a network, it is normal that your network administrator ping your computer from time to time. But if your computer is isolated, pings are rarer. One exception is if you have a DSL or cable connection; your ISP might ping your computer to check if it is on line.
- **Ping Broadcast Attacks**: No advanced settings.
- **Port Scans**: A slider lets you adjust the sensitivity from low to high in increments according to an internal calculation.
- **SYN Flooding**: Sensitivity, measured in number of attempted connections allowed per second.

Options

Click the Options button in the bottom-left corner of the Antivandal Policy screen to adjust additional Filtering settings.

The options appear in the pane to the right.



- **Stealth mode (prohibit ping replies)**: If this is checked, your computer will be invisible to other computers on the Internet or on a local network. You will not, however, be anonymous – any requests you send to other hosts will include your computer's IP address.
- **Stop unknown protocols**: If this is checked, VirusBarrier X6 automatically blocks any unknown protocols.
- **Deny Apple Remote Desktop Control**: If this is checked, VirusBarrier X6 blocks all access to your Mac by Apple Remote Desktop software.
- **Allow PORT mode FTP transfers**: If this is checked, you will be able to make FTP transfers when functioning in Client Only firewall mode.

The second part of this screen allows you to be notified by e-mail when an attack is detected. See later in this chapter, Understanding Alerts, for more information.

Unifying Policy Options

Each type of intrusion has settings that determine how you're alerted and what actions are taken when that type of intrusion is detected.

The "Use same policy for all types of protection" checkbox unifies all notifications and actions. With this box unchecked, you could, for example, choose to receive an e-mail when a buffer overflow attack is detected, but only see an alert box when an intrusion attempt occurs. Checking the box tells VirusBarrier X6 that you want to get the same sort of response no matter what type of intrusion occurs.

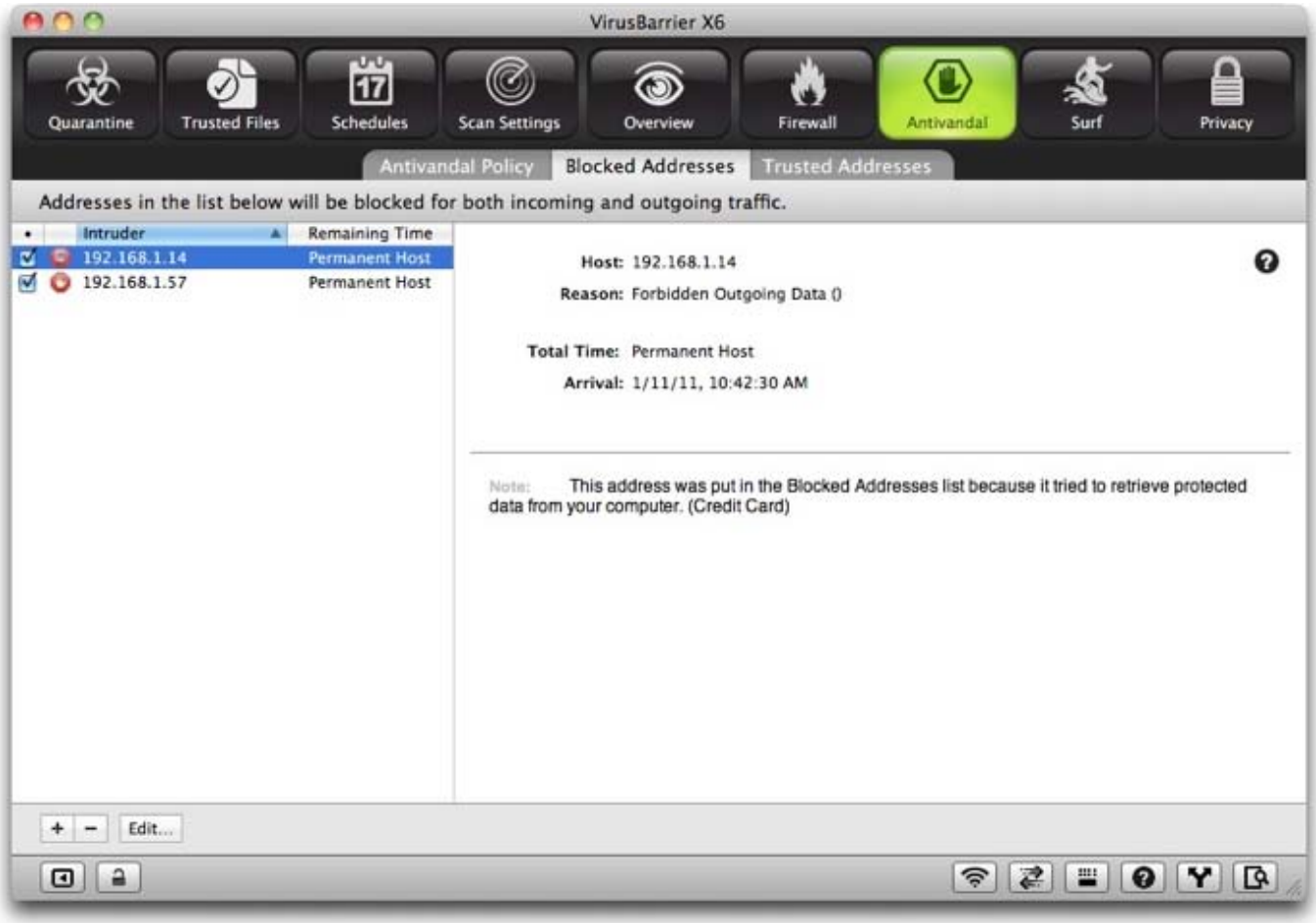
When you activate this option, you'll see a dialog box that asks which settings should become the model that other intrusion types will follow.

Blocked Addresses and Trusted Addresses

The Blocked Addresses list ensures that once an attempted attack or intrusion has been foiled, communication between the attacking machine and your Mac won't occur for a period of time that you define.

The Trusted Addresses list is the opposite of the Blocked Addresses list: it lists "friendly" computers that *are* allowed to connect to your Mac. While the Blocked Addresses list protects you from foes, the Trusted Addresses list opens the door to your friends. VirusBarrier X6's Antivandal tool will not block access to computers listed in the Trusted Addresses list, nor will it set off alerts for any actions they carry out. However, computers in the Trusted Addresses list will still be affected by all active Firewall rules.

The interface for the Trusted Addresses window is essentially the same as for the Blocked Addresses window, so we'll examine them both at the same time, pointing out differences as necessary. Here's the Blocked Addresses window.

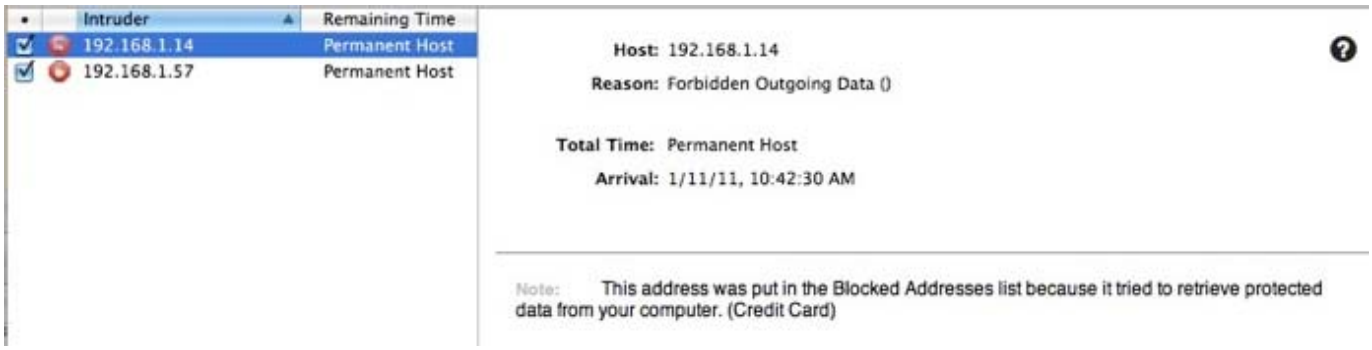


The panel on the left displays information about the various IP addresses that are currently in the Blocked Addresses list or Trusted Addresses list, if any.

- **Checkbox**: You can temporarily disable a Blocked/Trusted Address by unchecking this box, which is checked by default when you add a host to either list. When disabled, clicking it enables the item again. (This checkbox only appears if the IP address is set to be blocked permanently.)
- **Intruder/Host**: The second column shows the intruding IP address (in the Blocked Addresses list) or friendly IP address (in the Trusted Addresses list).
- **Remaining Time**: If you've set this IP address to be blocked or allowed for a specific period of time, this column shows how much time is remaining, updated every second. Otherwise, this column says "Permanent Host" to indicate that the IP address will be there until you remove it manually.

Blocked/Trusted Address Information

Clicking an item in the Blocked/Trusted Address lists shows some additional information on the right side of the panel. Double-clicking the item opens a new window with the same information.


Intruder
Remaining Time
192.168.1.14
Permanent Host
192.168.1.57
Permanent Host
Host: 192.168.1.14
Reason: Forbidden Outgoing Data ()
Total Time: Permanent Host
Arrival: 1/11/11, 10:42:30 AM
Note: This address was put in the Blocked Addresses list because it tried to retrieve protected data from your computer. (Credit Card)

- **Host**: The host's IP address. If you opened a new window by double-clicking the item, you can manually change the IP address listed. By clicking the DNS lookup button (the **?**), you can toggle from the numerical IP address to the actual domain name of the offender, if there is one. You can display this address in large type by moving your cursor over the word "Host", clicking, and selecting Large Type from the contextual menu that appears.
- **Reason**: Why the IP address was added to the Blocked Addresses list. This text doesn't appear in the Trusted Addresses list, as all items there are added manually.
- **Total Time**: The amount of time the host is to remain in the Blocked/Trusted Address list. Clicking the words **Total Time** changes the display to show Remaining Time; clicking again shows Elapsed Time, indicating how long the offender has been in the Blocked Addresses list. Clicking **Elapsed Time** will display the Total Time once again.
- **Arrival**: When the address was added to the Blocked/Trusted Addresses list.
- **Departure**: If you specified an amount of time for an IP address to remain in the Blocked/Trusted Addresses list, the time it will be released is given here.
- **Note**: Any comments you have entered for this IP address. VirusBarrier X6 will also automatically add comments to this field when it puts an item in the Blocked Addresses list, as in the example above.

A Note About DNS Lookups

In various places throughout VirusBarrier X6's interface you'll see a question mark in a dark circle. Clicking it toggles nearby information from a numerical IP address to its associated domain name and back again.

Be aware that IP addresses do not always have a one-to-one relationship to domain names. For example, a large domain might have www.example.com hosted on one IP address, forums.example.com hosted on another, and blog.example.com hosted on another.

Meanwhile, small domains often share one IP address with others, all hosted as "virtual domains" on a single computer. In such cases a domain lookup gives an IP address that actually leads to the larger, unexpected machine name, for example apache2-vat.market.example.com.

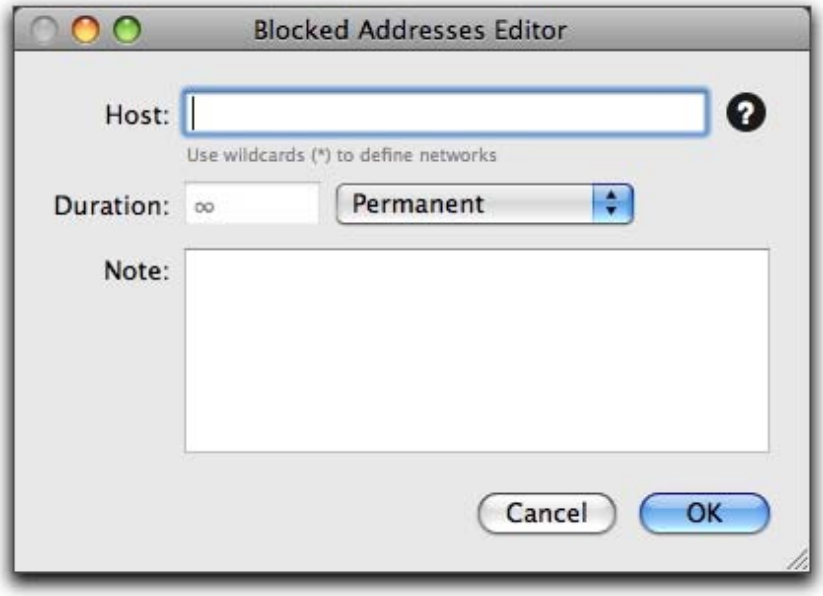
As a result, entering an IP address could block (or allow) traffic from unintended domains, while entering a domain might not block (or allow) all desired traffic. This is the nature of the Internet domain structure, and isn't an error of VirusBarrier X6. If you have problems with unexpectedly blocked or permitted traffic, try using a domain name instead of an IP address, or vice-versa.

Adding Addresses

There are two ways to manually add addresses to the Blocked Addresses list or Trusted Addresses list. (VirusBarrier X6 can also add addresses automatically to the Blocked Addresses list in response to Alerts. For more details, see later in this chapter, Understanding Alerts.)

The first way to add an address to the Blocked Addresses list or Trusted Addresses list is by selecting an IP address in the Log window and choosing **Add to Blocked Addresses** or **Add to Trusted Addresses** from the contextual menu. For more on this, see Using VirusBarrier X6 Monitoring Tools.

You can also manually add addresses to the Blocked/Trusted Addresses list by clicking the + button at the bottom of the list. A window appears.



Enter an IP address in the **Host** field, and select the time this address is to remain in the Blocked Addresses list or Trusted Addresses list by entering a number in the **Duration** field. Then, select a time unit from the popup menu. If you do not know the numerical IP address of the host you wish to add, enter its name and click the **?** button. VirusBarrier X6 queries your Internet provider's DNS server and enters the correct number in the field. You can also add comments, such as the reason for adding the address, in the **Note** field. If you decide you do not wish to add this address to the Blocked Addresses list or Trusted Addresses list, click Cancel.

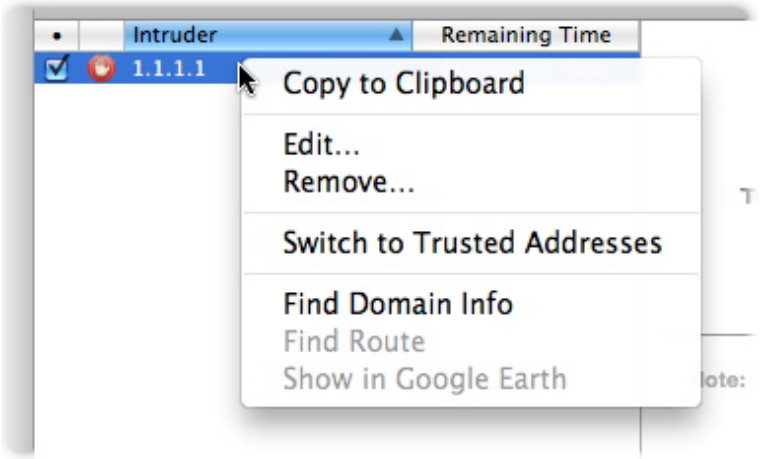
Using Wildcards

You can use wildcards to indicate ranges of IP addresses in the Blocked Addresses list or Trusted Addresses list. To do so, enter the first part of the IP address you wish to block, followed by asterisks, For example, 192.168.1.* will block all IP addresses from 192.168.1.0 to 192.168.1.255 inclusive; 192.168.*.* will block IP addresses from 192.168.[0-255].[0-255]; and so on.

Removing and Moving Addresses

To remove an address from the Blocked Addresses or Trusted Addresses list, click the address you want to remove, then click the - button.

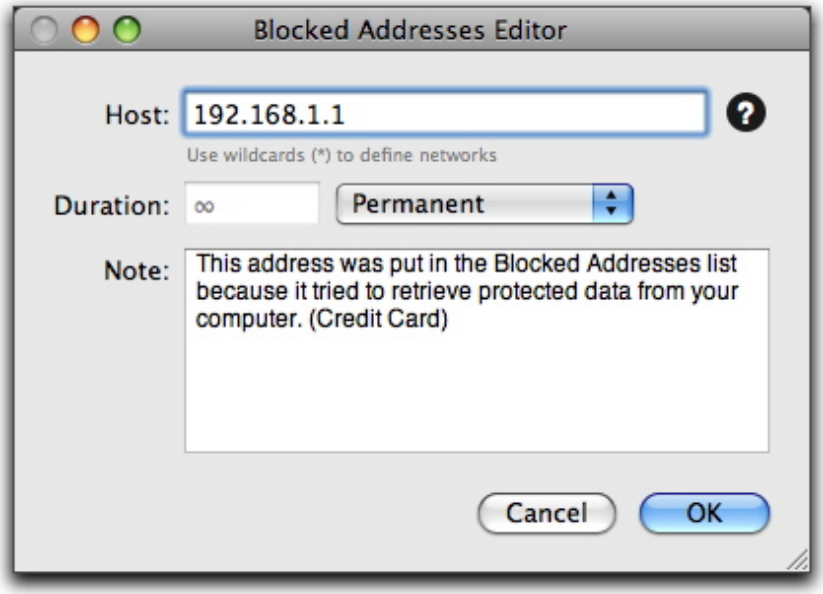
Another way to remove an address is by clicking it while holding down the Control key on your keyboard, then selecting **Remove...** from the resulting contextual menu. From this contextual menu, you can also move an address from the Blocked Addresses list to the Trusted Addresses list, or vice-versa.



Editing an Address

There are three ways to edit an address in the Blocked Addresses or Trusted Addresses list:

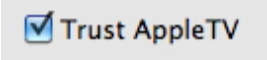
- Click the address you would like to edit, then click the **Edit...** button at the bottom left side of the pane,
- Double-click the address, or
- Click the address while pressing the Control key on your keyboard, then select **Edit...** from the contextual menu.



The Blocked/Trusted Addresses Editor window appears. You can change the address, add or change comments, or change the amount of time you want the item to remain on the Blocked/Trusted Addresses list.

Trusting an AppleTV

There is one option available in the Trusted Addresses list that is not present in the Blocked Addresses list: **Trust AppleTV**. The AppleTV is a device made by Apple that serves as a set-top portal to movie and TV show rentals from the iTunes Store, and that can also stream music and videos from an iTunes library on any Mac or PC. The AppleTV has a particular way of acting on the network, and in some cases VirusBarrier X6 would see this as a threat because of the way it polls computers. Checking **Trust AppleTV** on the Trusted Addresses list ensures that VirusBarrier X6 does not see your AppleTV as hostile.



Note: if you have trusted IP addresses on your local network, by adding 192.168.1. to the Trusted Addresses list, and the AppleTV is on the same network, you won't need to check this option.*

The Contextual Menu

As you have seen above, you can click an item in the Blocked/Trusted Addresses list while pressing the Control key on your keyboard to raise a contextual menu. There are four functions in this menu that have not yet been discussed: **Copy to Clipboard**, **Find Domain Info**, **Find Route**, and **Show in Google Earth**.

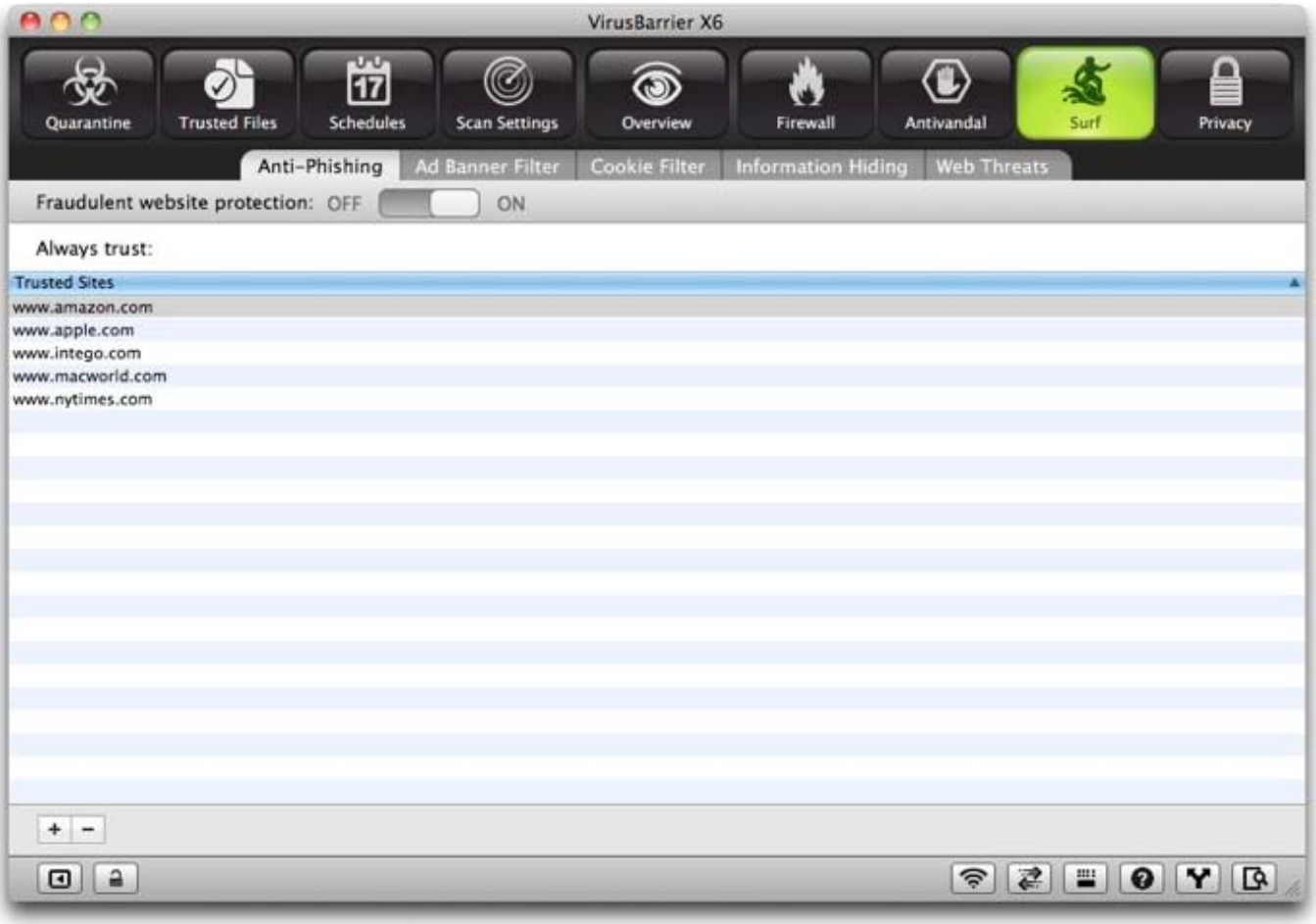
- **Copy to Clipboard**: Puts the IP address on the Mac OS X Clipboard, where it can be pasted into other programs, such as a text editor.
- **Find Domain Info**: Opens VirusBarrier X6's Whois window and performs a search on the selected IP address. See Using VirusBarrier X6 Monitoring Tools.
- **Find Route**: Opens VirusBarrier X6's Traceroute window and performs a search on the selected IP address. See Using VirusBarrier X6 Monitoring Tools.
- **Show in Google Earth**: Launches the Google Earth program, if you have it installed, and attempts to find the geographic location of the selected IP address.

Surf Filters

VirusBarrier X6 provides protection against phishing, web threats (threats that arise from booby-trapped web pages), as well as providing three filters that help you control the information your Mac sends and receives while surfing the Internet.

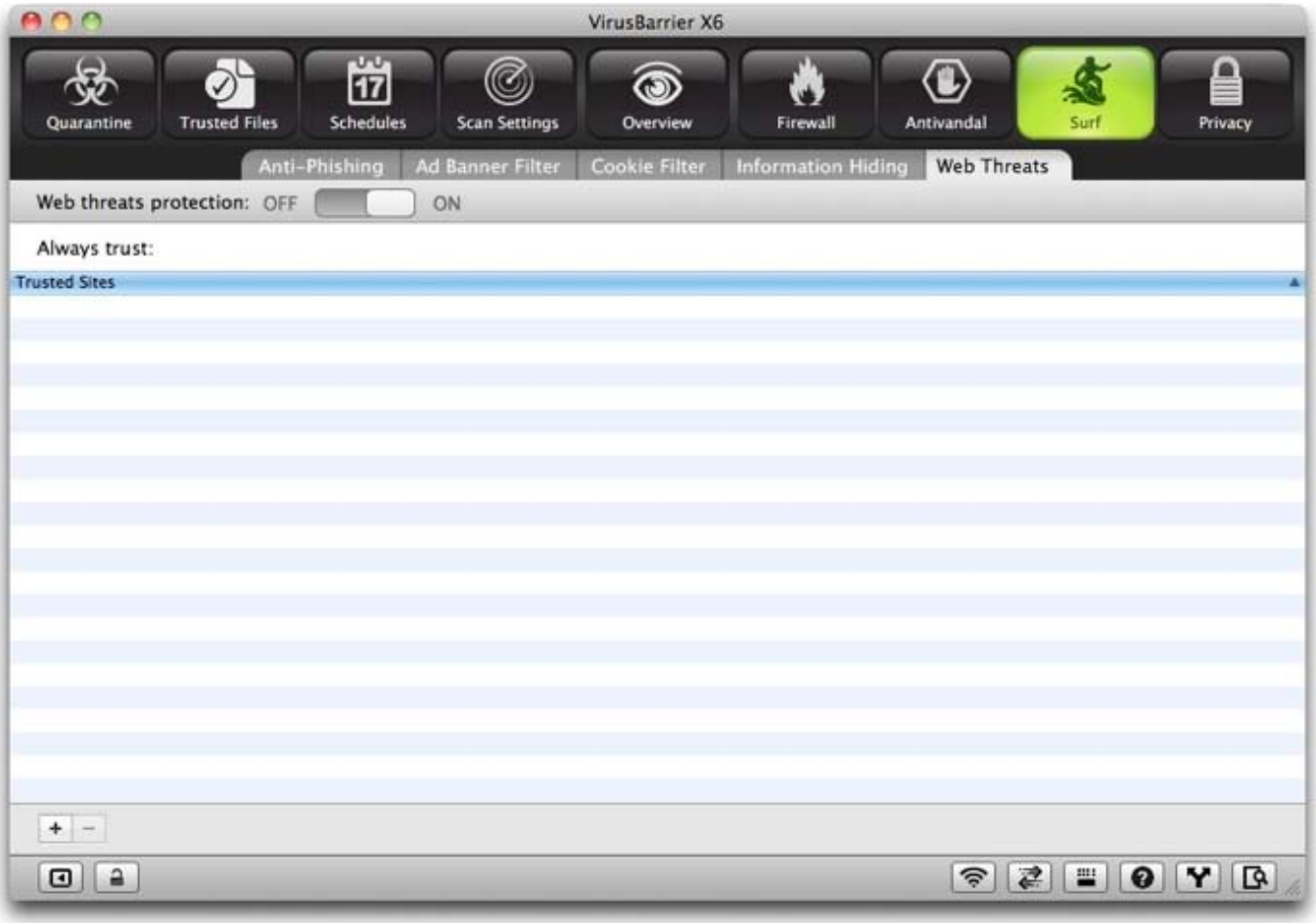
To see VirusBarrier X6's Surf settings, click the Surf button.

VirusBarrier X6's Anti-Phishing protection keeps you safe from phishing (attempts to trick you into entering personal information on bogus web sites that impersonate real sites). VirusBarrier X6 blocks such sites, protecting you from this type of scam. Nevertheless, you should never click a link in an unsolicited e-mail message if you have doubts about its veracity.



To activate VirusBarrier X6's Anti-Phishing protection, move the **Fraudulent website protection** slider to **ON**. You can manually add sites that you always want to trust by clicking the + button at the bottom of the window, then typing the URL of a site you trust. The only reason you might want to do this is if certain sites are incorrectly flagged as being phishing sites.

VirusBarrier X6 offers protection from web threats, such as cross-site scripting attacks, drive-by downloads, clickjacking, as well as web pages with malicious JavaScript or malicious Java applets.



To activate VirusBarrier X6's Web Threat protection, move the **Web threats protection** slider to **ON**. You can manually add sites that you always want to trust by clicking the + button at the bottom of the window, then typing the URL of a site you trust. The only reason you might want to do this is if certain sites are incorrectly flagged as being malicious.

Three other Surf filters help you choose what type of information you want to send about your Mac to web servers, and help keep your surfing ad-free:

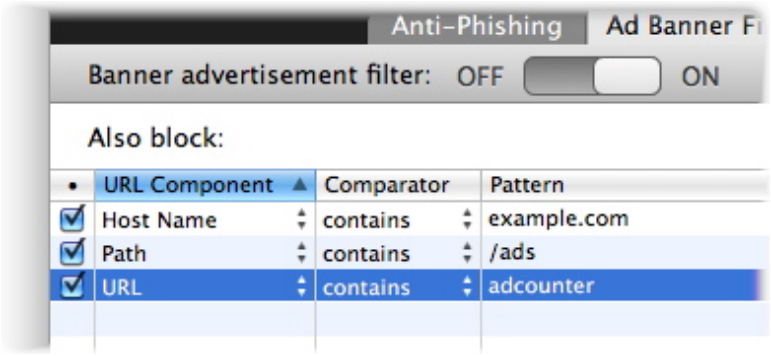
- The **Ad Banner Filter** hides ad banners on web sites that you visit;
- The **Cookie Filter** prevents your Mac from sending certain information to web sites that track your movements;
- The **Information Hiding** filter cloaks certain facts about your Mac, web browser, and the last web site you have visited.

Surf filters affect all computer programs that communicate using the HTTP protocol. Web browsers are the most common programs using HTTP, but it's also part of iTunes, RSS newsreaders, and a lot of other software that has Internet browsing capabilities. If you have unexpected difficulties with such programs – downloading music through iTunes, or accessing specific RSS feeds, for example – try disabling the surf filters temporarily.

Ad Banner Filter

The Ad Banner Filter is a list of rules that VirusBarrier X6 uses to filter unwanted web material such as graphic ads known as "ad banners," helping you surf much faster and with less distraction. VirusBarrier X6 blocks these ads, and replaces them with tiny, transparent graphics. VirusBarrier X6 contains an internal list of ad banner strings to filter, but you can also add custom strings to filter more ads you encounter when surfing.

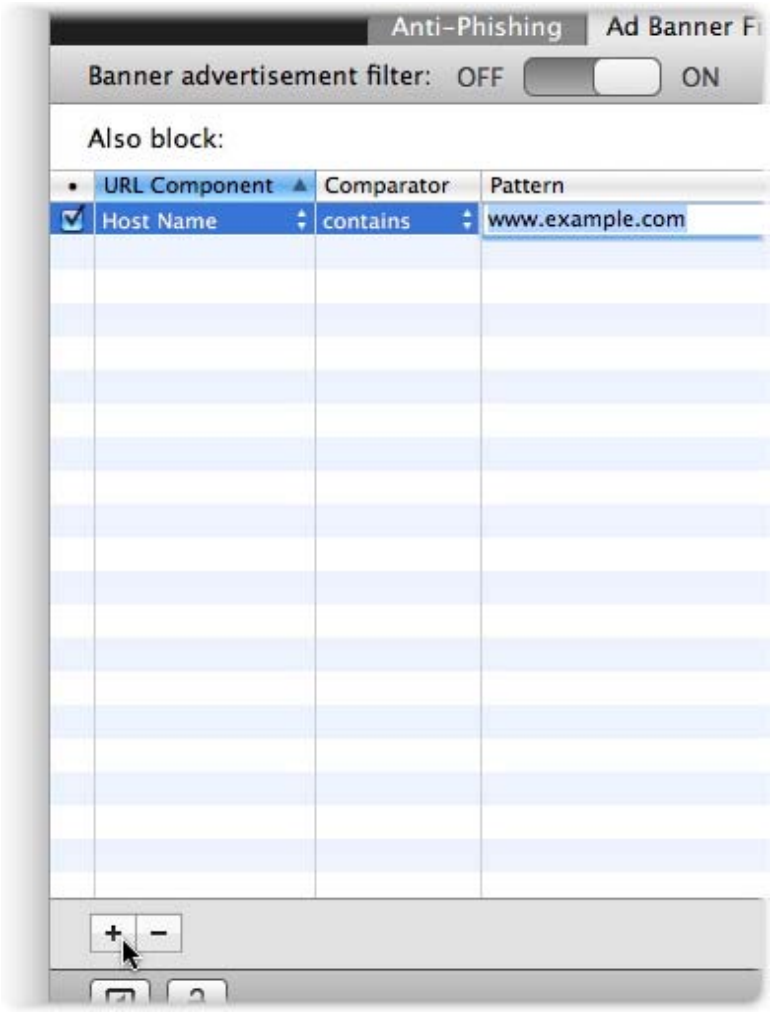
Click the Ad Banner Filter tab to view the filter window. Here it is, populated with sample data:



To enable the Ad Banner filter, move the **Banner advertisement filter** slider to **ON**.

Adding Rules to the Ad Banner Filter

The Ad Banner filter already contains a set of rules, which is kept up-to-date when you update your VirusBarrier X6 Filters but you can easily add your own. To add rules to the Ad Banner filter, click the + button. A new line is added to the ad banner list for you to edit.



The list contains four columns: a checkbox, **URL Component**, **Comparator** and **Pattern**. The pattern, obviously, is how you define what you want blocked.

The URL Component popup menu has three options. VirusBarrier X6 searches each ad banner filter in the selected element:

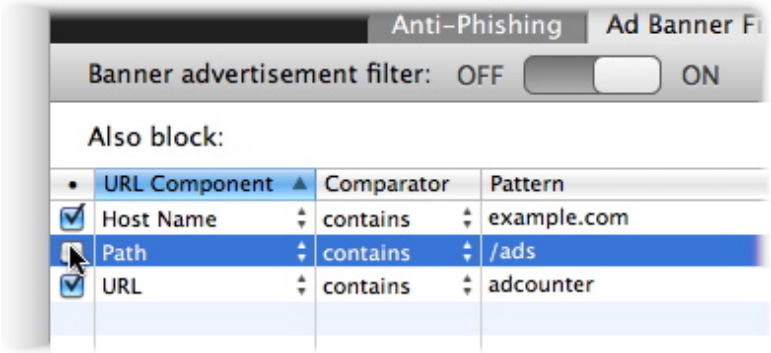
Host Name: The Internet domain – that is, anything in a Web address between the http:// and the first following "/". The default value is www.example.com. Note that such an entry wouldn't block (for example) http://forums.example.com; to block both, you should simply enter example.com.

- **Path**: Any part of the URL following the host name, such as /ads/ in http://www.example.com/home/graphics/ads/6542.html.
- **URL**: The entire URL, such as http://www.example.com/home/graphics/ads/6542.html.

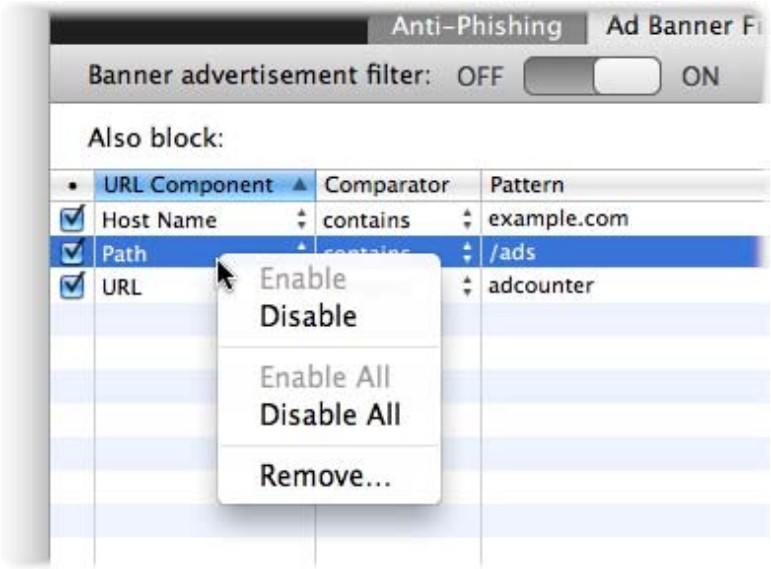
The **Comparator** popup menu lets you choose whether content should be blocked based on an exact match ("is") or when your text matches at least a portion of the URL ("contains").

Activating or Deactivating Ad Banner Rules

Each ad banner rule appears on a line in the Ad Banner window. A checkbox at the left of each line allows you to activate or deactivate the filter for each ad banner rule. When you add a new ad banner rule, the box is checked, indicating that the filter is active for this rule. To stop blocking certain ad banners, uncheck the checkboxes for the ad banners in question.



You can also enable ad banner blocking for an individual ad banner rule, or for all ad banner rules, by holding down the Control key on your keyboard and clicking the name of an ad banner rule. A contextual menu displays.



Select Dis**Pattern**able to disable protection for the selected ad banner rule, or select **Disable All** to disable protection for all ad banner rules. (If the Rule was already disabled, the **Enable** and **Enable All** choices would be available.)

To remove ad banner rules, either choose the Remove option in the contextual menu or click the – button below the list of ad banner rules.

Note that the Ad Banner filter doesn't know what content it's filtering, only that the URL matches the criteria you

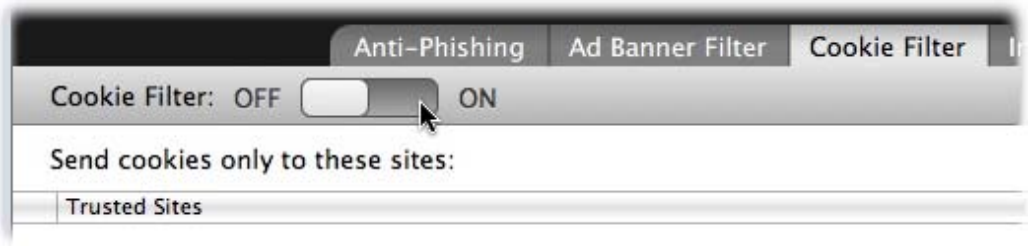
specified. Therefore, you might occasionally have difficulty seeing information on Web pages that coincidentally match your criteria, but aren't actually ad banners. If this is the case, try turning off the Ad Banner filter temporarily. You can do this from the VirusBarrier X6 application, or from the Intego menu in your menubar.

Cookie Filter

VirusBarrier X6 includes a Cookie Filter, which prevents your Mac from sending tracking information, called "cookies," to all web sites except for those you specify.

The Cookie Filter is useful when you want to surf in extreme privacy, only telling a few, trusted sites about your actions. However, many Web sites – particularly those that require a password – won't work correctly unless you specifically include them in the list of trusted sites.

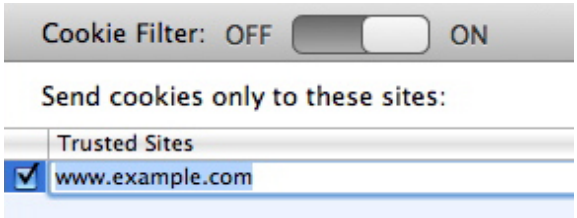
To turn on the Cookie Filter, click the Cookie Filter tab and move the **Cookie Filter** slider to **ON**.



You'll see a warning that certain sites won't function properly unless you add them to the Trusted Sites list. Click **OK** to continue.

Enabling this option may prevent you from accessing web sites that require Cookies to be enabled.
Access to accounts on sites such as Facebook, YouTube or Amazon may be blocked if these sites are not in the Trusted Sites list.
OK

To add a server to the Cookies Filter list, click the + button at the bottom of the list. A dummy server address (www.example.com) displays: change it to the site of your choice.

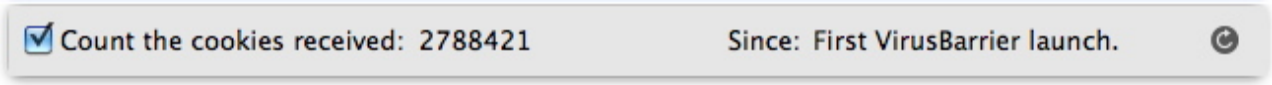


Erase the dummy server address and enter the name of the server you want to allow cookies to be sent to. You can also drag a URL from a browser, or even a URL in text format, to this field to add it to the list.

As with the Ad Banner filter, you can enable or disable individual servers by clicking the checkboxes next to them, or by holding down the Control key while clicking on them and using the contextual menu, or clicking with your right mouse button.

Cookie Counter

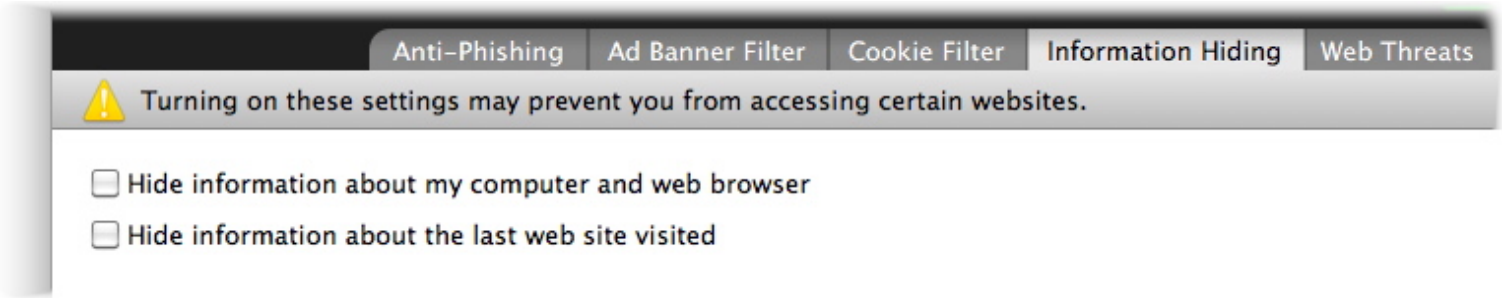
VirusBarrier X6 can also count the number of cookies for all users on your Mac, if you check the **Count the cookies received** checkbox at the bottom of the cookies filter screen. A display tells you how many cookies your Mac has accepted since you first installed VirusBarrier X6, or last reset the counter. At any time you can reset the counter to zero by clicking the small arrow to the right.



Information Hiding

All Web browsers reply to requests from web sites, telling which platform you are using (Mac, Windows, Linux, etc.) and which browser and version you are using. This information can help the site deliver information in the best way, for example by turning on features that only work for the Web browser that you're using. On the other hand, some sites limit access by platform and browser, in some cases forbidding access to everybody using a Mac. VirusBarrier X6 can hide some information concerning your computer, possibly permitting access where it would otherwise be denied.

To see and change Information Hiding settings, click the Information Hiding tab.


Anti-Phishing
Ad Banner Filter
Cookie Filter
Information Hiding
Web Threats
Turning on these settings may prevent you from accessing certain websites.
Hide information about my computer and web browser
Hide information about the last web site visited

Check the **Hide information about my computer and web browser** checkbox to reply to such web site requests by sending only generic information. For example, your computer will reply to the web site that you're using a Mozilla browser, but with no version number or platform.

Some sites also keep track of the last site you visited. Again, this can improve your web experience if, for example, a shopping site offers you discounts if you come from a specific Web site. But unscrupulous sites might use this feature to follow your browsing habits in ways you don't want. By checking the **Hide information about the last web site visited** checkbox, VirusBarrier X6 prevents your Mac from replying to this type of request.

Privacy Protection

VirusBarrier X6's privacy protectors examine both incoming and outgoing data packets, looking for specific types of data and helping protect your privacy. To see and change your Privacy settings, click the Privacy button.

Anti-Spyware

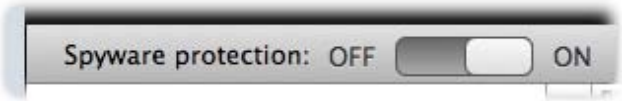
VirusBarrier X6 lets you control access from your Mac to the Internet and local networks by individual applications.

While your firewall settings may allow general network access, the Anti-Spyware tab lets you choose how VirusBarrier X6 reacts when specific applications try to access the network. This helps you in two ways:

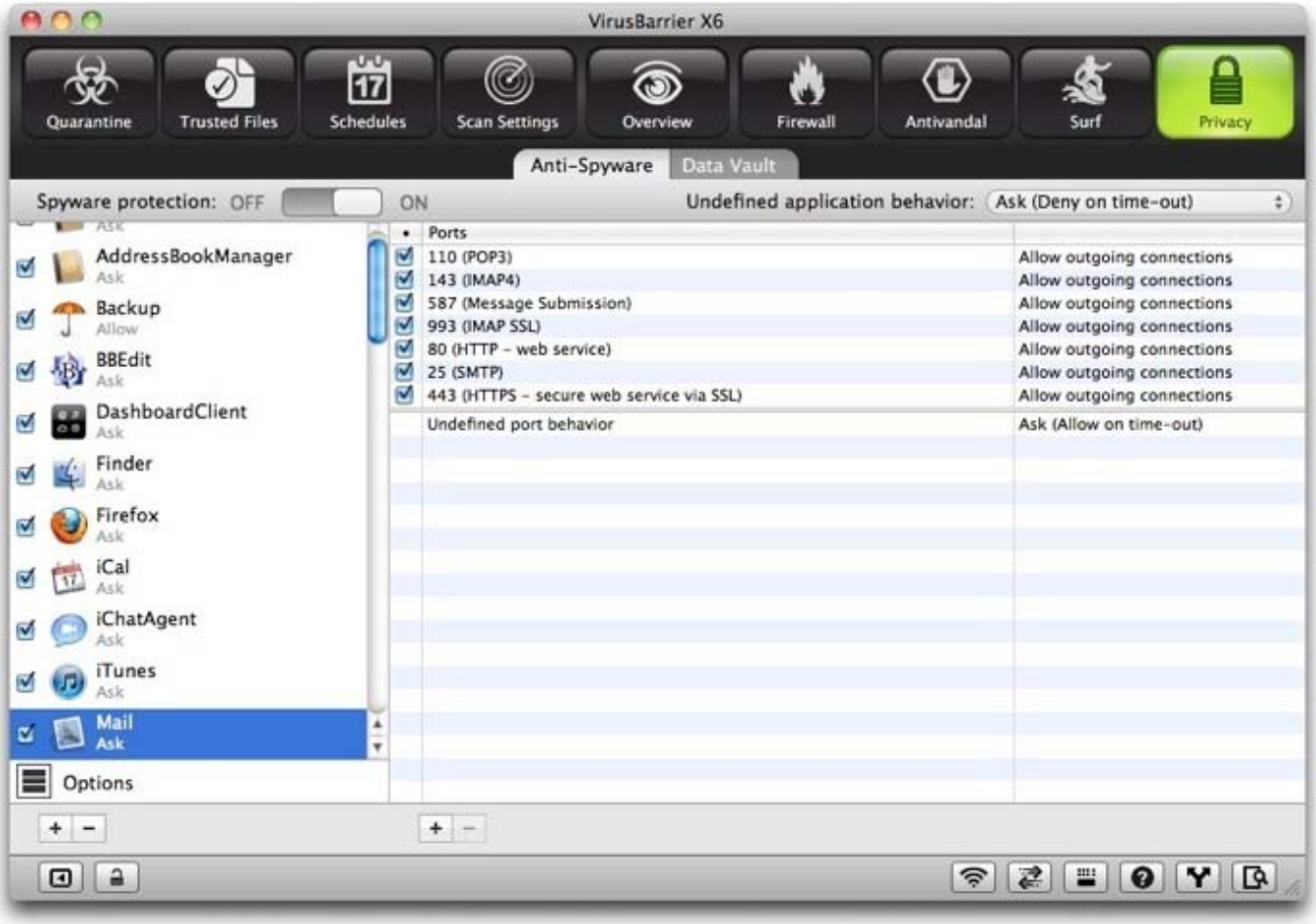
- You can prevent users from accessing the network with specific applications.
- If an application attempts to connect to the network behind your back, VirusBarrier X6 stops it in its tracks, alerts you, and waits for you to decide whether to allow it to do so or to block it.

Your Mac has many applications that access the Internet or other networks, including web browsers, e-mail programs, FTP (file transfer) programs and instant messaging applications. But there may also be programs that connect to the network without telling you, in order to verify the serial numbers of software installed on your computer, collect and send personal information without your awareness, or open a backdoor on your Mac to provide access to hackers or vandals. VirusBarrier X6 notifies you of such attempts and allows you to decide whether to allow them.

To turn on the Anti-Spyware feature, move the Spyware protection slider to **ON**.



Anti-Spyware works by first asking you to make a list of applications for which you want to apply settings. These are known as "defined" applications, while all those that aren't on the list are "undefined". In the following example, Safari is defined, while the Firefox web browser (which isn't on the list) is undefined.

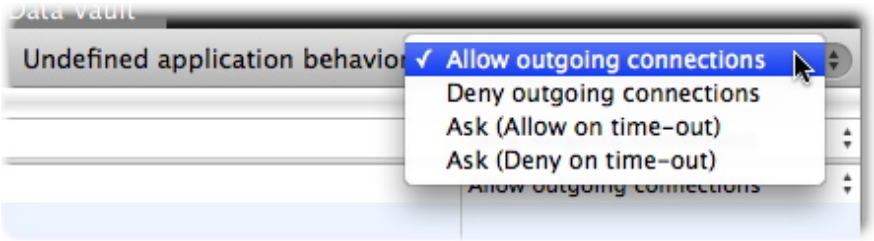


Once you've built this list, you can finely control communications from defined applications and set a general policy for communications from undefined applications. Two typical configurations would be:

- You run a computer lab and want people to be able to send e-mail using Apple's Mail program, but not browse

the Web or play network games. You would define Mail as Allowed, but deny all outgoing connections from other programs.
- You suspect that an application you downloaded to your Mac is sending unauthorized communications, perhaps from hidden spyware built into the program. You define that program and deny all communications from it, but allow all communications from undefined applications.

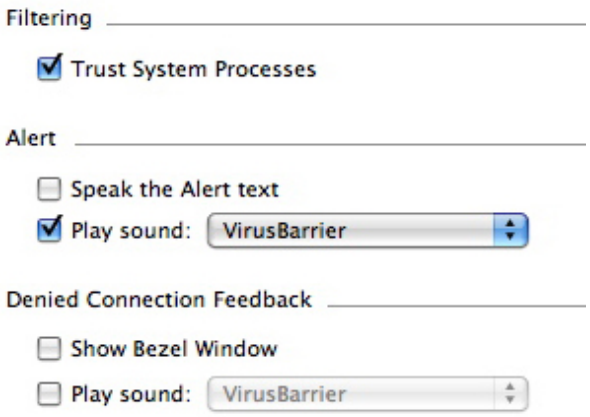
Four behavior options are available for undefined applications:



- **Allow outgoing connections**: VirusBarrier X6 allows all applications to access the Internet or any other network. However, any firewall rules you may have defined concerning access to and from specific ports still function. For example, if an FTP program attempts to connect to a Web page, VirusBarrier X6 does not block the application, but if you have set up a firewall rule blocking port 20, the standard FTP port, the data does not go through. If the FTP program attempts to make a connection to a different port, it is not blocked.
- **Deny outgoing connections**: VirusBarrier X6 blocks all access to the Internet or other networks. This supersedes all firewall rules you have defined.
- **Ask (Allow on time-out)**: VirusBarrier X6 asks you for each application that attempts to connect to the Internet or other network. If you do not respond within 90 seconds, the application will be allowed to access the Internet, but only this time.
- **Ask (Deny on time-out)**: VirusBarrier X6 asks you for each application that attempts to connect to the Internet or other network. If you do not respond within 90 seconds, the application will be denied access, but only this time.

Options

The Options button in the lower-left corner of the Anti-Spyware pane allows you to configure some general Anti-Spyware settings.



The one option that's special to Anti-Spyware is **Trust System Processes**, which allows communications from the many parts of Mac OS X itself that request Internet or network access. Such requests might relate to printing services, domain name resolution, checks for software updates or clock synchronization. These are requests that come from parts of Mac OS X, not separate applications. To trust these processes, and not be asked when they attempt to connect

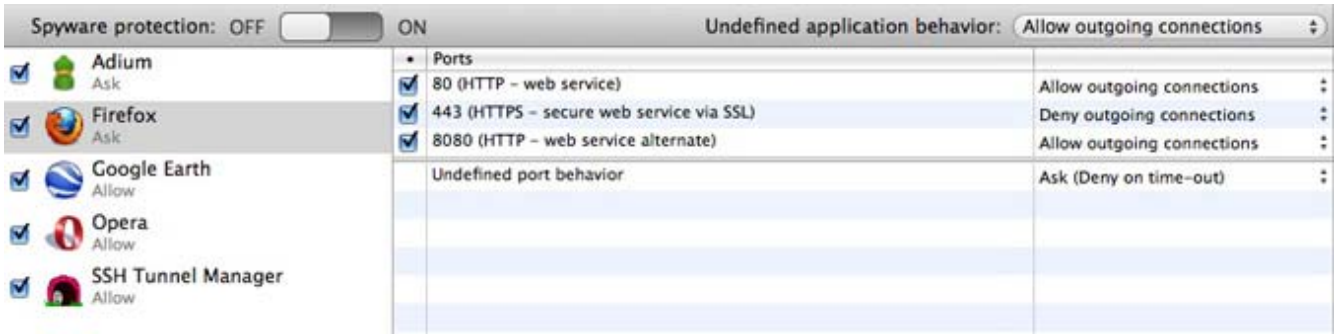
to the Internet or network, check the **Trust System Processes** checkbox.

The other options relate to alerts and feedback when connections are blocked. Choose those that suit the way you want to be alerted to unauthorized or blocked connections. For more about these options, see Understanding Alerts later in this manual.

Applications: Adding, Removing and Changing Settings

After you have chosen to allow or deny network access to undefined applications, define an application by clicking the + button, then navigating through the Mac OS X dialog box to the application itself to add it. (You can also add applications by dragging their icons from the Finder.) Repeat the process for all the applications you wish to add. To remove an application from the list, click it and then click the - button at the bottom of the application list.

You can then change the settings for each application to allow or block communications from the application as a whole, or over specific ports. Similar to the process above, where you specify what should happen when undefined applications attempt outgoing communications, here you define what you'd like to happen when a specific application attempts communication from an undefined port. Then you define a list of ports for that specific application that are exceptions to the general rule.



In the above example:

- Five applications (listed on the left) have specific rules governing them; outgoing connections are allowed from all other applications.
- Firefox is permitted to send two kinds of communications, via ports 80 and 8080.
- Communications by Firefox via port 443 are forbidden.
- Communications by Firefox via any other port raise an alert on your Mac's screen; if you don't respond to allow the communication within 90 seconds, it is denied.

This list of ports contains three columns:

- The first column, containing checkboxes, indicates the port behavior that is currently activated for the application. If the box next to a port is checked, the behavior you have specified is active. If you want to deactivate this behavior, then uncheck the box. You can reactivate it later by checking the box.
- The second column, Ports, provides information on the ports that the application uses to access the network. It tells you the port number, and, in some cases, the protocol used and a brief description. (This description appears automatically when you enter a port number that VirusBarrier X6 recognizes.) You can add a port number, or a range of port numbers, for example 110-123.
- The third column contains either "Allow outgoing connections" or "Deny outgoing connections." You can change from one to the other at any time by clicking the text.

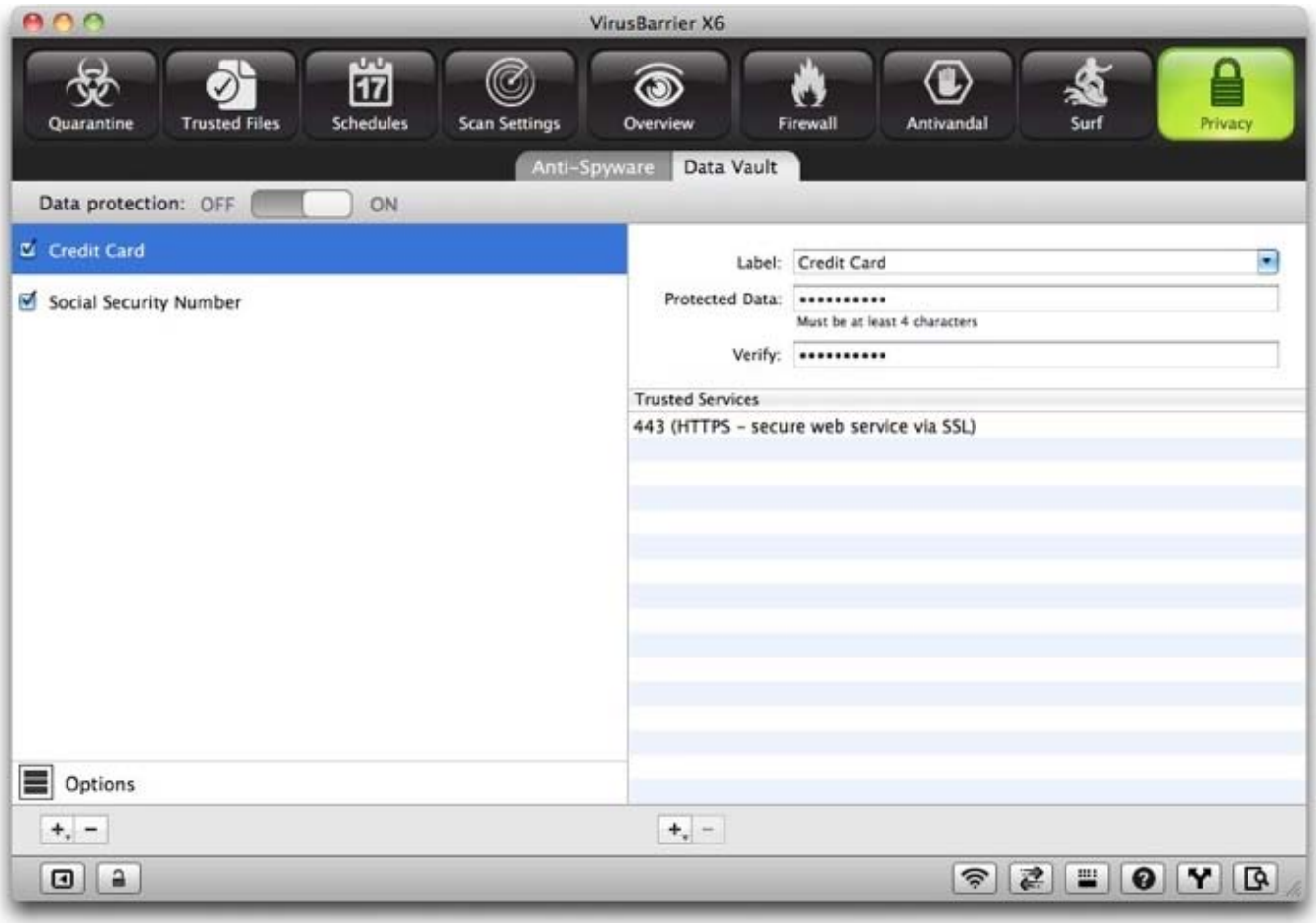
To view an application on the Applications list in the Finder, hold down the Control key on your keyboard and click on the name of an application. A contextual menu appears. Select Show in Finder, and a Finder window opens revealing the location of the application. This helps you find applications that were added following alerts or time-outs.

Note: one way to use the Anti-Spyware feature of VirusBarrier X6 is to turn it on and have the program ask you whether to allow applications to connect to the Internet. Each time this happens - only once per application, and per port - you'll add the applications you want to allow, and slowly build up your list. By doing this, however, you'll see just how many applications connect to remote servers. Bear in mind that, for many applications, these connections are merely to check for updates, as many programs have built-in update features. VirusBarrier X6 has no way of knowing what type of information is being sent or requested.

Data Vault

The Data Vault ensures that any sensitive information you choose to protect cannot leave your Mac and go onto a network. You decide what to protect - your credit card number, passwords, or key words that appear in sensitive documents - and VirusBarrier X6's data filter checks each outgoing packet to make sure that no documents containing this information are sent. Not only does this protect you from accidentally sending documents containing this information, but it also protects against anyone who has network access to your Mac from taking copies of them.

To reach the Data Vault pane, click the Privacy button then click the Data Vault tab.



How the Data Vault Works

VirusBarrier X6 examines all data packets that are sent from your computer to the Internet or a local network. If any of the data you indicated in the filter is found, the packet is blocked.

The Data Vault only blocks data that corresponds *exactly* to the text you indicated, including punctuation and case. For example, if you entered your credit card number as protected data, VirusBarrier X6 prevents it from leaving your computer and can warn you in several ways if you choose. But if you enter the same number in a secure web page,

your browser encrypts this number. The data therefore no longer corresponds to the protected data, and is sent. The same is true for data that is encoded in other manners, or compressed.

In extremely rare instances, the Data Vault stops data that matches your criteria but not your intention. For example, graphic files (such as images on web sites) are essentially just strings of data thousands of characters long. It's possible that a graphic file could coincidentally contain a piece of data you want protected, and would therefore be blocked by the Data Vault. (If you decided to block the name "Jodie", for example, a graphic file containing the string "Cg34gb$sEbOJodie8%" would be stopped.) If you find yourself unable to send or receive a specific piece of information, try turning off the Data Vault momentarily, then turn it on after the information has been transferred.

Move the **Data protection** slider in the upper-left corner to **ON** to enable the Data Vault. You can turn it off at any time, for example to temporarily allow your protected data to be sent. You can also turn it off through the Intego menu in your menubar.

What to Protect

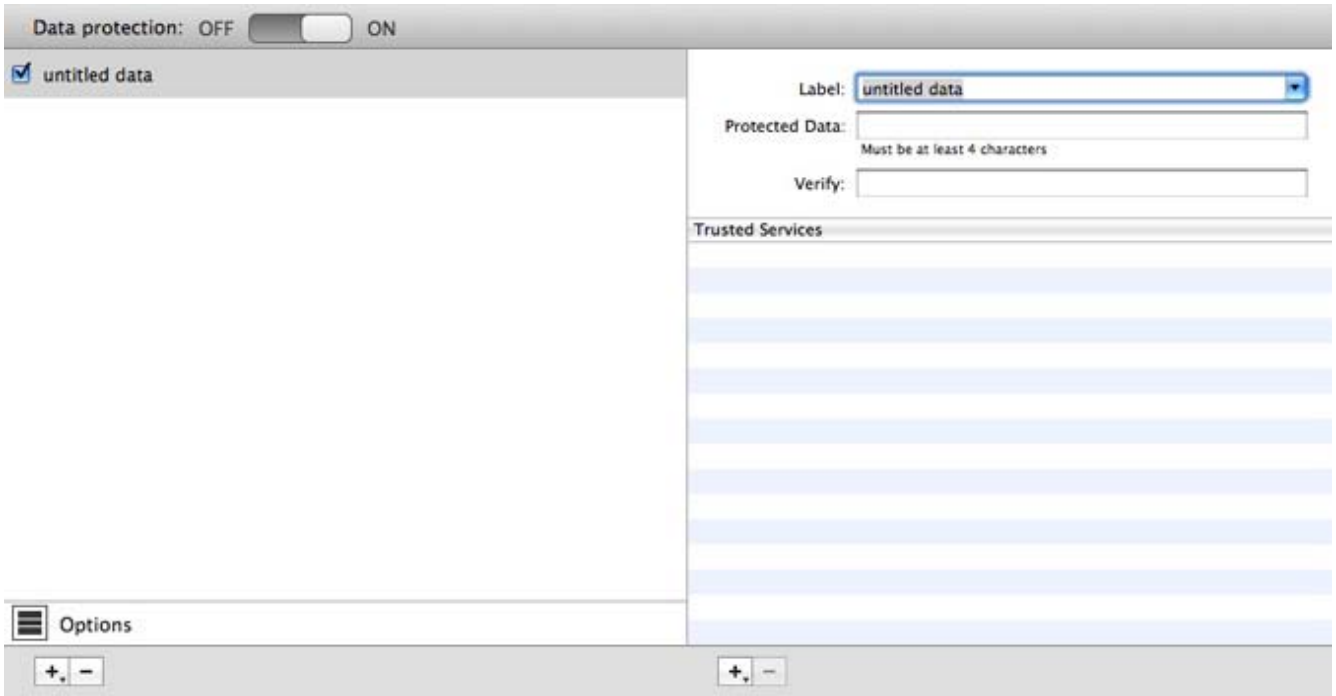
The Data Vault includes labels for the six most common types of sensitive information:

- **Credit Cards**
- **E-mail Addresses**
- **Home Addresses**
- **Names**
- **Social Security Numbers**
- **Telephone**

However, these labels are merely for convenience. VirusBarrier itself doesn't treat these types differently from one another, or differently from any additional types you might decide to enter later – for example, "Wall-safe combination," "Children's names" or "Passwords."

Adding Data to the Vault

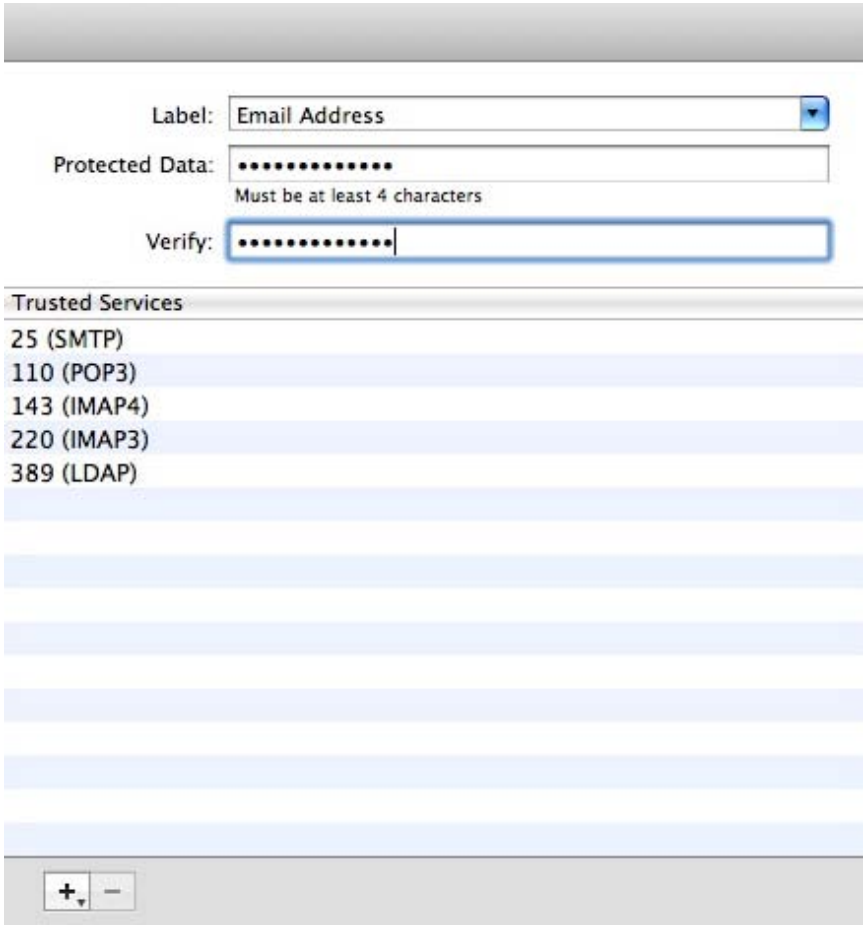
To add data to the Data Vault, click the + button below the **Options** icon. A new entry named "untitled data" appears in the filter list.



Enter a description for your protected data in the **Label** field, or choose it from the popup menu: you'll notice that it is echoed in the vault list. Then enter the actual data you wish to protect in the **Protected Data** field. This text is hidden so nobody watching over your shoulder or who later has access to your Mac can see it. You must enter the data a second time in the **Verify** field. If the **Protected Data** and **Verify** fields do not match, a window displays, giving you the choice of either resetting the protected data, in which case you will have to retype both data fields, or clicking **OK**. If you click **OK**, you will have to retype the verified protected data.

You must enter your text *exactly* as it will be found in your documents for the filter to protect it. For example, a credit card number may be found as ####-####-####-#### or as #### #### #### ####. If you protect only the first example, the filter does not look for the second one. Also, this data is case sensitive. If you need to protect a key word, such as a project name, you must enter it in all possible cases that you may use: i.e., Marketing Study, marketing study, MARKETING STUDY.

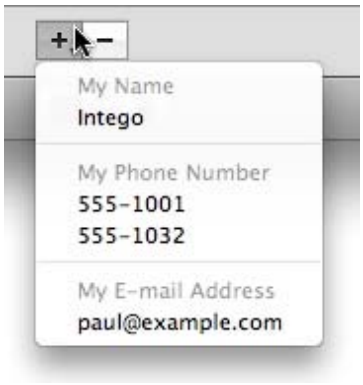
The **Trusted Services** section allows you to choose to block data for all but the selected services. To do this, click the + button below the Trusted Services list. Then, type the port number of the service. Alternately, click the + sign and hold the mouse button down for a few seconds: you'll be able to choose from a popup list of common services. (Some of them, such as Mail in the example below, add several ports in one go.) You can add a single port number, or a range of port numbers, for example 110-123. Data to this port (or these ports) will not be blocked. To add another service, repeat the above operation. You can add as many services as you wish.



You can also drag and drop services from the Services Library. This is particularly helpful if you do not know the specific port numbers you wish to add to the list. To display the Services Library, choose **Window** > **Services Library**, or press Option-Command-6. Select the desired service, then drag it onto the **Trusted Services** list.

You can add certain personal information from your card in Apple's Address Book, if you have filled one out. To do this, click and hold the + button below the Data Vault list in the left column, and you'll see items divided into three

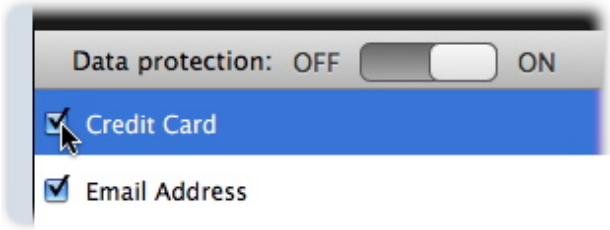
groups: My Name, My Phone Number and My E-mail Address. Select one of these to add it as protected data.



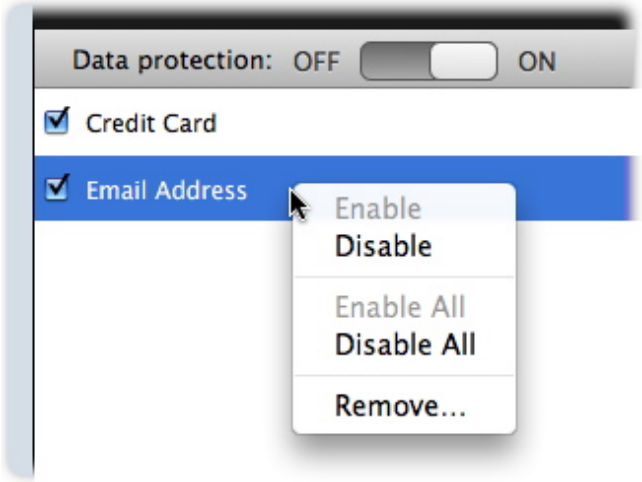
Once you have finished entering this information, your data is protected. You can go back at any time to edit the data item by clicking on it in the Data Vault list and changing information in its pane to the right.

Activating, Deactivating and Deleting Data Items

Each item of protected data appears on a line in the Data Vault window. A checkbox at the left of each line allows you to activate or deactivate the filter for each data item. When you add a new data item, the box is checked, indicating that the filter is active for this item. If you wish to send that data over the Internet or a local network, you must uncheck the checkbox for the item in question, or deactivate all the Data Vaults by moving the **Data protection** slider to **OFF** as mentioned earlier.



You can also activate or deactivate Data Filters for individual protected data items, or for all protected data items, by holding down the Control key on your keyboard and clicking the name of a data item, or by clicking with your right mouse button. A contextual menu displays.

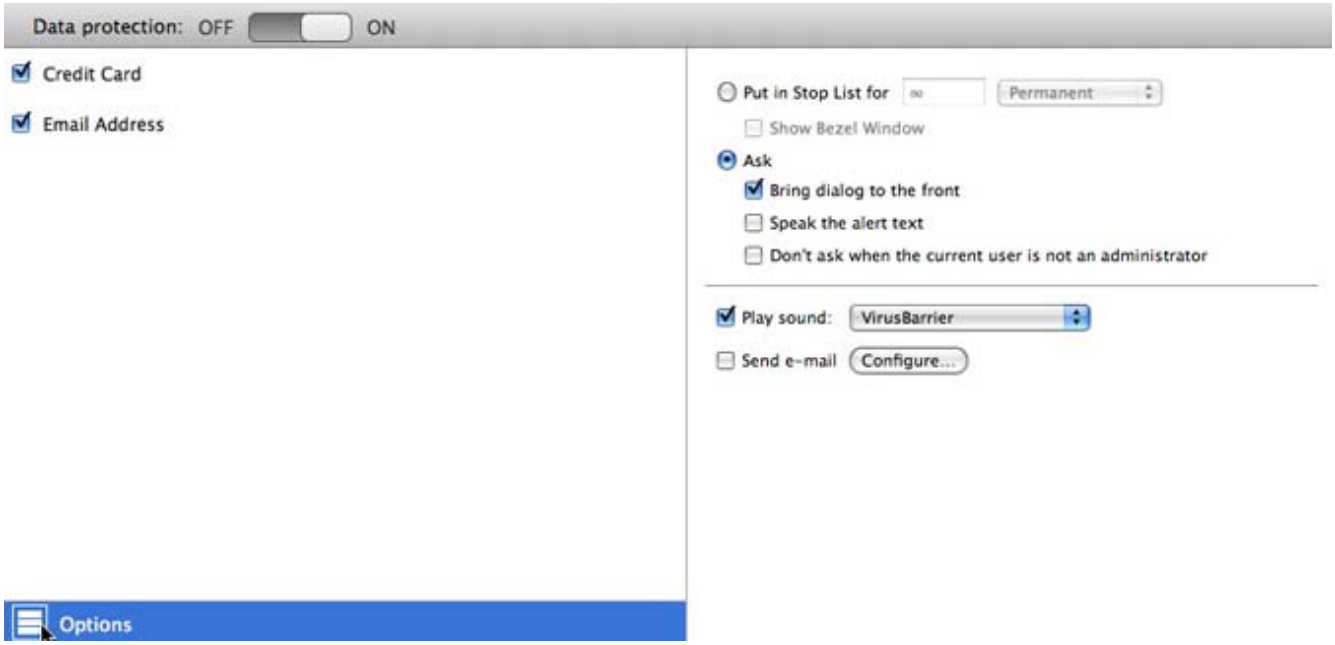


Select **Disable** to disable protection for the selected data item, or select **Disable All** to disable protection for all data items. (If the selected item in the above example had been disabled already, the choices for **Enable** and **Enable All** would be available.)

If you'd like to permanently remove the item from the Data Vault list, either Control-click as described above and choose **Remove...**, or select the data item and click the - button. In either case, a dialog box asks you to confirm that you really want to remove the data item.

Data Vault Options

When protected data attempts to enter or leave your Mac, you have several options as to how you're notified, and what to do about future attempts. To see these options, click the **Options** button in the lower-left of the data screen. Changes to Data Vault options affect all Data Vaults.



To understand these options, see the next section, Understanding Alerts.

Understanding Alerts

VirusBarrier X6 constantly monitors your computer's network activity to both the Internet and local networks, and will look out for specific types of data that indicate an intrusion or attack. If any suspicious data is found, VirusBarrier X6 displays an alert, asking you whether you wish to allow the data to be sent or deny it. Just like the malware alerts explained in Protecting Your Mac from Viruses and Malware, VirusBarrier X6 displays alerts when certain network events occur.

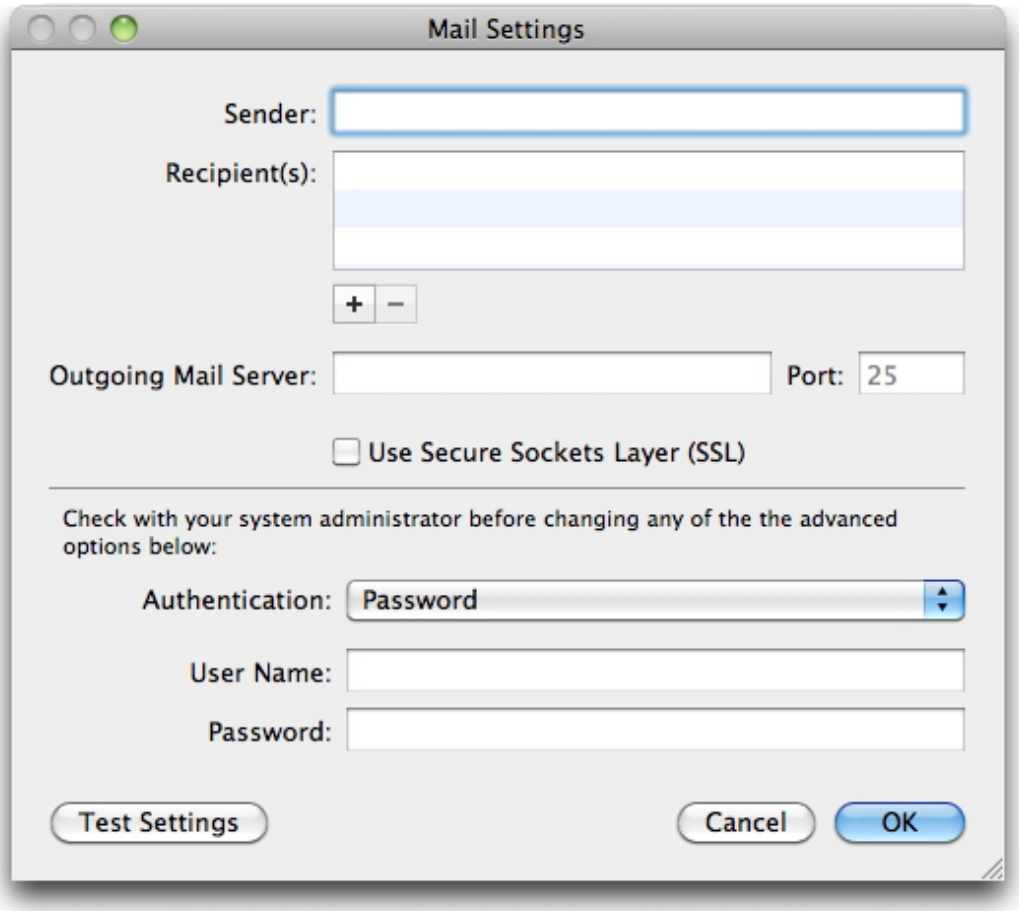
Alert Settings

Network alerts are displayed when certain network events occur. This includes when Trojan horses are spotted, when protected data is being sent from your Mac, when the Anti-Spyware feature detects an undefined application attempting to connect to the Internet, when the firewall blocks data and more.

Settings for these alerts appear in several places throughout VirusBarrier X6, as is described in relevant sections of this manual. To understand these settings better, we'll look at them as they appear in the **Antivandal Policy** section.

- **Put in Blocked Addresses**: If this radio button is on, the connection is automatically dropped when there is an alert, and the offending IP address is immediately placed in the Blocked Addresses list. A field to the right of this button allows you to specify the default time period that the offending IP address will remain in the Blocked Addresses list. You can choose any number of seconds, minutes, hours or days, or put the intruder in the Blocked Addresses list permanently. (Results from checking the **Show Bezel Window** checkbox are shown in the section below, "Examples of Alerts.")
- **Ask**: If this radio button is on, VirusBarrier X6 presents an alert dialog asking what to do. When an alert appears, it shows the Blocked Addresses time period selected by default, but this time can be changed in Policy tab for each type of attack. In addition, you have three options:
    - **Bring dialog to the front**: The alert comes to the front automatically whenever there is an alert. If not, it remains in the background. If you take no action within 90 seconds, the alert automatically closes, and the connection is denied.
    - **Speak the alert text**: VirusBarrier X6 uses Mac OS X's Text-to-Speech feature to speak the text of the alert.
    - **Don't ask when the current user is not an administrator**: VirusBarrier X6 only gives the above options if the Mac OS X user has administrator's privileges. Otherwise, it automatically puts the offending host in the Blocked Addresses list.
- **Play sound**: VirusBarrier X6 plays the sound of your choice whenever there is an alert. You can select the sound you want from the popup menu to the right of the button. (The sound plays once when you make a selection.)
- **Send e-mail**: VirusBarrier X6 automatically sends an e-mail message to the address configured in the **Options** panel, within 30 seconds. (VirusBarrier X6 waits to see if there are other intrusion attempts, rather than sending an e-mail message each time.)

If you've requested e-mail notification, you must configure your e-mail settings to receive any alert notifications by e-mail. In the **Policy** section, you do that by clicking **Options**, then clicking the **Configure...** button.



You must enter e-mail addresses for the **Sender** and **Recipient(s)**, as well as the **Outgoing Mail Server**. Further, you'll need to enter a username and password that your mail server will accept. E-mail messages can be sent to multiple recipients. To add a recipient, click the + button. To remove a recipient, click the - button.

Examples of Alerts

The following is an example of an alert when the **Put in Blocked Addresses** radio button is selected and the **Show Bezel Window** checkbox is enabled.

As you can see, you're given no options, only a notification. If the **Show Bezel Window** checkbox had been disabled, you'd have seen nothing, and VirusBarrier X6 would have silently added the IP address to the Stop List.

Here's an example of an alert when the **Ask** radio button is on, and the **Bring dialog to the front** checkbox is enabled.

VirusBarrier X6
Alert: Forbidden Outgoing Data (Credit Card)
From Host: 192.168.1.14
Put this host in the Blocked Addresses for
∞
Permanent
More Info...
Ignore
Block Address
When: Tuesday, January 11, 2011 12:17:41 PM Europe/Paris +0100
Details: VirusBarrier just stopped protected data from being sent. If you really want to send this data, click ignore. Otherwise, the data will not be sent, and your correspondent will be added to the blocked addresses list.

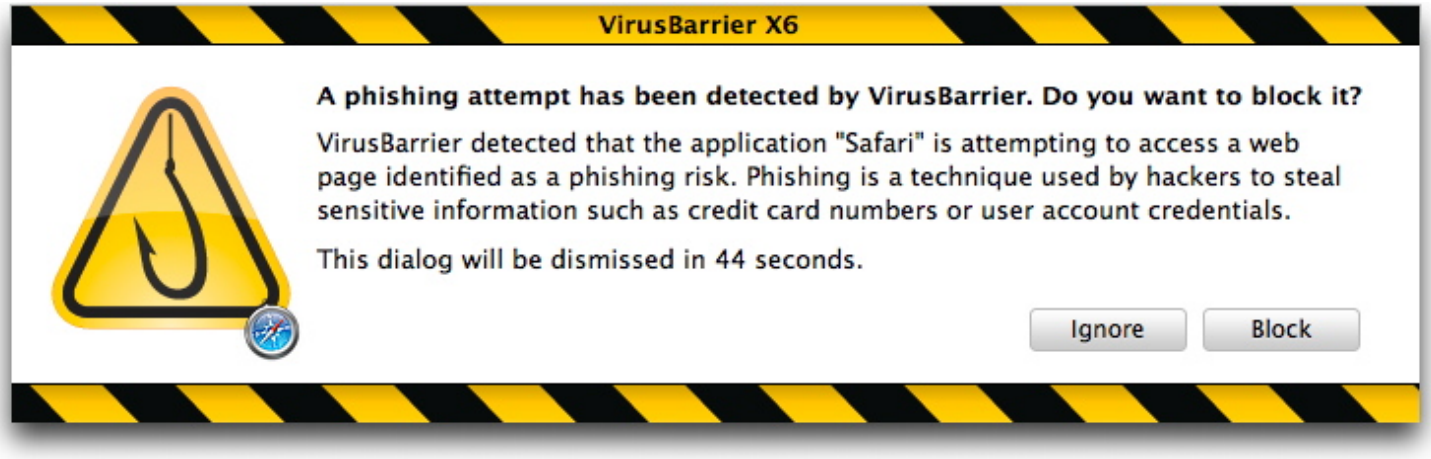
The top line shows the reason for the alert. The host is given as an IP address, but you could find out its associated domain name (if any) by clicking the "?" icon. We've already clicked the disclosure triangle to show **Details**, which gives further information.

Two buttons allow you to decide what action to take for this alert.

- **Ignore**: if you click this button, you will allow the data to be sent. Data transmission will continue as usual, unless VirusBarrier X6 detects another attempted intrusion, in which case another alert will appear.
- **Block Address**: if you click this button, the data being transferred will be refused and the intrusion will be blocked. When this happens, the packet is dropped, and it is as if the data was never transferred. If the suspicious packet is part of a file, this means that the file will not reach its destination. If it is a command, the command will not have a chance to be carried out, since it will not reach its target. In addition, the IP address that caused this alert will be automatically added to the Blocked Addresses list, and kept there for the default time that has been set. You can make changes to this time in the popup menu.

Here's an example of an alert that occurred when an application attempted to reach the Internet in violation of Anti-Spyware rules.

Finally, here's the type of alert you'll see when VirusBarrier X6 thwarts a phishing attempt. You have the option of blocking the site or ignoring it and visiting the site; do the latter at your own risk.


VirusBarrier X6
A phishing attempt has been detected by VirusBarrier. Do you want to block it?
VirusBarrier detected that the application "Safari" is attempting to access a web page identified as a phishing risk. Phishing is a technique used by hackers to steal sensitive information such as credit card numbers or user account credentials.
This dialog will be dismissed in 44 seconds.
Ignore
Block

‹‹ Protecting Your Mac from Viruses and Malware

Using VirusBarrier X6 Monitoring Tools ››

© 2011 Intego. All Rights Reserved.

Using VirusBarrier X6 Monitoring Tools

- The VirusBarrier X6 Log
- Traffic Monitors
- Viewing Active Services
- Viewing Network Information
- Whois Queries
- Traceroute Searches

Go to Main Table of Contents

VirusBarrier X6 contains a number of monitoring tools to help you see which actions the program has carried out on malware, to record network activity and intrusion attempts, and to give you an overview of your Mac's activity in real time. From the log, which shows both malware scan results and network activity, to the VirusBarrier Traffic Monitor, which shows current network throughput, these tools and others help you manage your Mac and its network activity.

The VirusBarrier X6 Log

To access the VirusBarrier X6 log , click the small "magnifying glass" icon at the bottom of the screen, choose **Window > Logs**, or press Command-Option-L.

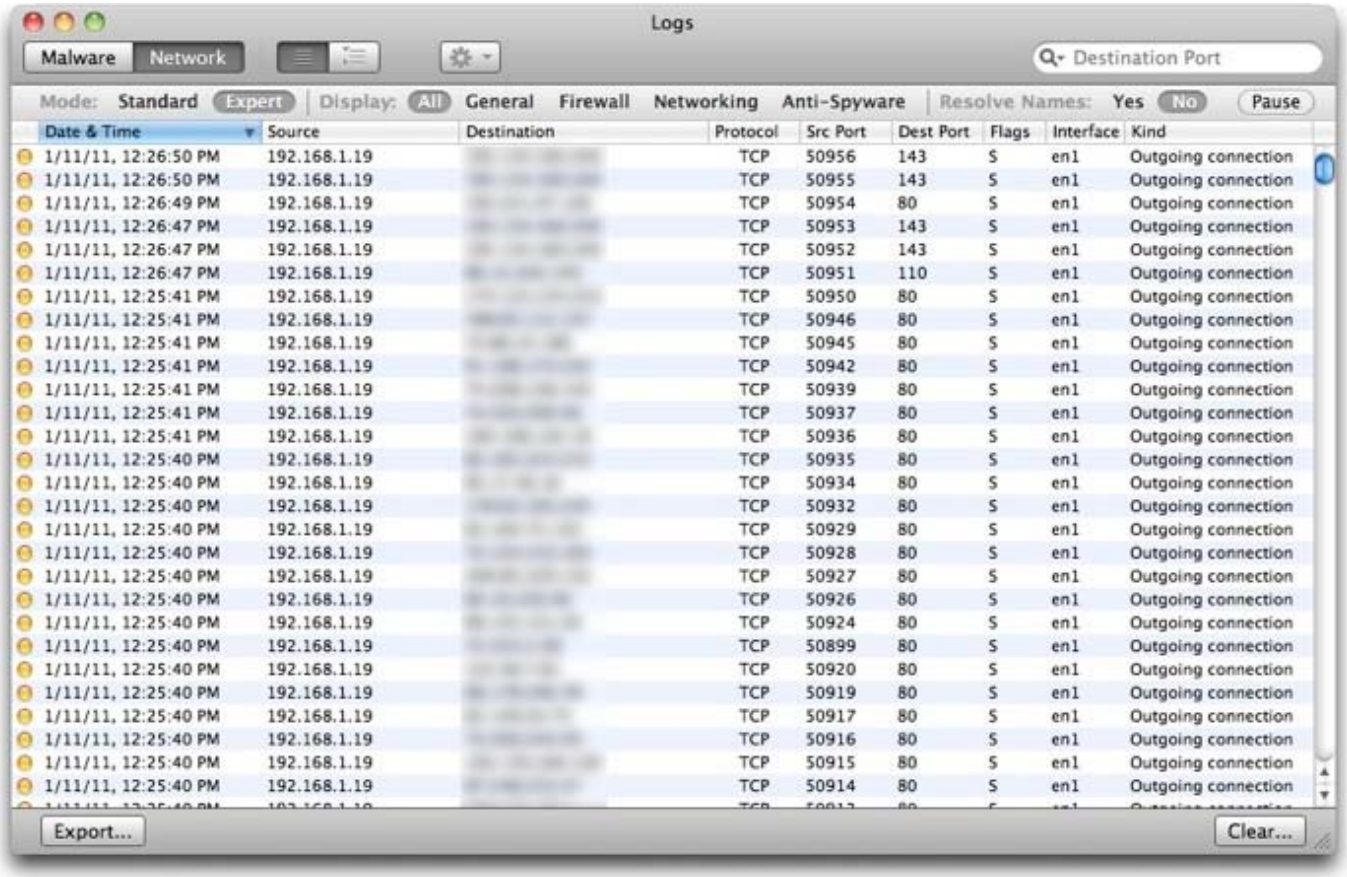
When the log window displays, you'll see two buttons at the top-left: **Malware** and **Network**. You can view either of these two logs by clicking the appropriate button.

The Network Log

The network log shows a record of all network activity that VirusBarrier X6 has observed, as well as all intrusion attempts that VirusBarrier X6 has blocked. You can apply filters to it on several criteria to highlight issues of interest.

To access the network log, click the Network button in the top-left corner of the Log window, if it isn't already selected.

You'll see the network log window. Of course your entries won't be the same as those shown here, but rather will reflect activity on your Mac since you installed VirusBarrier X6 (or last cleared the log).


Logs
Malware
Network
Destination Port
Mode: Standard Expert
Display: All General Firewall Networking Anti-Spyware
Resolve Names: Yes No
Pause
Date & Time
Source
Destination
Protocol
Src Port
Dest Port
Flags
Interface
Kind
1/11/11, 12:26:50 PM 192.168.1.19 TCP 50956 143 S en1 Outgoing connection
1/11/11, 12:26:50 PM 192.168.1.19 TCP 50955 143 S en1 Outgoing connection
1/11/11, 12:26:49 PM 192.168.1.19 TCP 50954 80 S en1 Outgoing connection
1/11/11, 12:26:47 PM 192.168.1.19 TCP 50953 143 S en1 Outgoing connection
1/11/11, 12:26:47 PM 192.168.1.19 TCP 50952 143 S en1 Outgoing connection
1/11/11, 12:26:47 PM 192.168.1.19 TCP 50951 110 S en1 Outgoing connection
1/11/11, 12:25:41 PM 192.168.1.19 TCP 50950 80 S en1 Outgoing connection
1/11/11, 12:25:41 PM 192.168.1.19 TCP 50946 80 S en1 Outgoing connection
1/11/11, 12:25:41 PM 192.168.1.19 TCP 50945 80 S en1 Outgoing connection
1/11/11, 12:25:41 PM 192.168.1.19 TCP 50942 80 S en1 Outgoing connection
1/11/11, 12:25:41 PM 192.168.1.19 TCP 50939 80 S en1 Outgoing connection
1/11/11, 12:25:41 PM 192.168.1.19 TCP 50937 80 S en1 Outgoing connection
1/11/11, 12:25:41 PM 192.168.1.19 TCP 50936 80 S en1 Outgoing connection
1/11/11, 12:25:40 PM 192.168.1.19 TCP 50935 80 S en1 Outgoing connection
1/11/11, 12:25:40 PM 192.168.1.19 TCP 50934 80 S en1 Outgoing connection
1/11/11, 12:25:40 PM 192.168.1.19 TCP 50932 80 S en1 Outgoing connection
1/11/11, 12:25:40 PM 192.168.1.19 TCP 50929 80 S en1 Outgoing connection
1/11/11, 12:25:40 PM 192.168.1.19 TCP 50928 80 S en1 Outgoing connection
1/11/11, 12:25:40 PM 192.168.1.19 TCP 50927 80 S en1 Outgoing connection
1/11/11, 12:25:40 PM 192.168.1.19 TCP 50926 80 S en1 Outgoing connection
1/11/11, 12:25:40 PM 192.168.1.19 TCP 50924 80 S en1 Outgoing connection
1/11/11, 12:25:40 PM 192.168.1.19 TCP 50899 80 S en1 Outgoing connection
1/11/11, 12:25:40 PM 192.168.1.19 TCP 50920 80 S en1 Outgoing connection
1/11/11, 12:25:40 PM 192.168.1.19 TCP 50919 80 S en1 Outgoing connection
1/11/11, 12:25:40 PM 192.168.1.19 TCP 50917 80 S en1 Outgoing connection
1/11/11, 12:25:40 PM 192.168.1.19 TCP 50916 80 S en1 Outgoing connection
1/11/11, 12:25:40 PM 192.168.1.19 TCP 50915 80 S en1 Outgoing connection
1/11/11, 12:25:40 PM 192.168.1.19 TCP 50914 80 S en1 Outgoing connection
Export...
Clear...

Network Log View Options

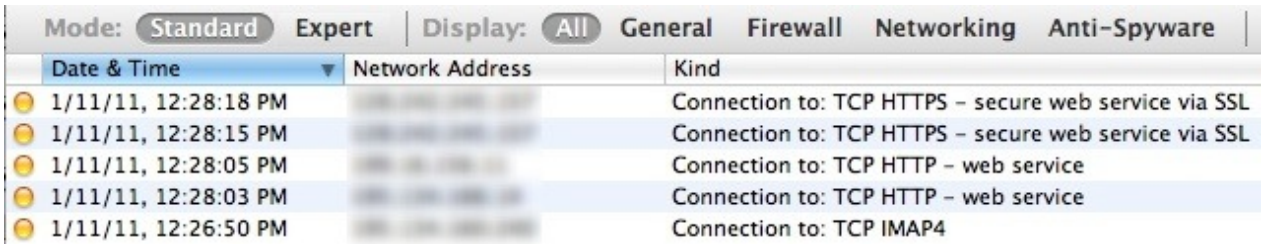
The top of the log window contains three groups of options that affect how the log appears.

- The first group toggles between the default Standard view and an extended Expert view;
- The second group shows subsets of log activity to help you see potential issues more clearly;
- The third group lets you choose whether to view raw IP addresses or domain names using DNS lookup.

We'll examine each of these sets of options separately.

Standard and Expert Log Views

Standard: The default view for the Log screen. This displays only four pieces of information for each Log entry.


Mode: Standard Expert
Display: All General Firewall Networking Anti-Spyware
Date & Time
Network Address
Kind
1/11/11, 12:28:18 PM
Connection to: TCP HTTPS – secure web service via SSL
1/11/11, 12:28:15 PM
Connection to: TCP HTTPS – secure web service via SSL
1/11/11, 12:28:05 PM
Connection to: TCP HTTP – web service
1/11/11, 12:28:03 PM
Connection to: TCP HTTP – web service
1/11/11, 12:26:50 PM
Connection to: TCP IMAP4

- Type of activity, indicated by dot color:
  - Yellow: Notable event, such as an outgoing connection, incorrect login, blocked outgoing data, etc.
  - Red: Network attack, blocking of address in the Blocked Addresses list, Anti-Spyware blocking, etc.
- **Date & Time** of activity, according to your Mac's clock setting.
- **Network Address**, given by default as an IP address. If you've checked **Resolve Names** (see below), you'll see the domain names for those addresses that VirusBarrier X6 was able to resolve.
- **Kind**, a short description of the activity.

Expert: An extended view, shows the following additional fields where applicable.

Mode: Standard Expert
Display: All General Firewall Networking Anti-Spyware
Resolve Names: Yes No
Pause
Date & Time
Source
Destination
Protocol
Src Port
Dest Port
Flags
Interface
Kind
1/11/11, 12:28:18 PM 192.168.1.19 TCP 50960 443 S en1 Outgoing connection
1/11/11, 12:28:15 PM 192.168.1.19 TCP 50959 443 S en1 Outgoing connection
1/11/11, 12:28:05 PM 192.168.1.19 TCP 50958 80 S en1 Outgoing connection
1/11/11, 12:28:03 PM 192.168.1.19 TCP 50957 80 S en1 Outgoing connection
1/11/11, 12:26:50 PM 192.168.1.19 TCP 50956 143 S en1 Outgoing connection

- **Source**, which is the originating IP address (or domain) of the incident. For most activities, the source will be your Mac's IP address, although for attacks or other incoming connections it will be that of the remote computer. If you have checked Resolve Names, you will see the domain names for those addresses that VirusBarrier X6 was able to resolve.
- **Destination**, given by default as an IP address.
- **Protocol**, which describes how the connection was attempted, i.e. TCP, UDP, ICMP or IGMP.
- **Source Port**, the port from which data was sent.
- **Destination Port**, the intended port for the data.
- **Flags**, or TCP flags: A (acknowledge), S (synchronize), F (end of data), or R (reset).
- **Interface**, the network interface used to send the data, such as Ethernet or AirPort, given by BSD Name.
- **Kind**, a short description of the activity.

Viewing Subsets of the Network Log

Activities fall into four groups: General, Firewall, Networking and Anti-Spyware. You can choose to see activities relating to all the groups at once, or only activities relating to a specific one. Click one of the buttons to change the log view.

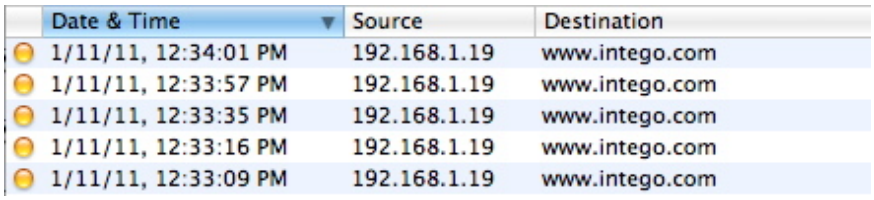
- **All**: All activity that VirusBarrier X6 tracks. This is the default setting.
- **General**: Activity related to the operation of VirusBarrier X6 itself, such as instances when you launched and quit the program, added applications to Anti-Spyware, entered items into the Blocked Addresses or Trusted Addresses list, and so forth.
- **Firewall**: Incidents when network activity triggered a firewall rule, if logging was turned on for that rule. Records of any Trojan horse attacks also appear in the Log, if you've turned on Trojan protection.
- **Networking**: All connections to networks or the Internet, and when IP addresses in the Blocked Addresses list attempt to connect to your computer.
- **Anti-Spyware**: A subset of the General group, showing only when applications were added to or removed from

the Anti-Spyware list, or when Anti-Spyware rules were called into play.

Resolving Domain Names in the Network Log

VirusBarrier X6 helps you track down intruders by resolving the domain names of your connections. Internet addresses exist in two forms: IP numbers, such as `192.168.1.1`, and names, such as `example.com`. The correspondence between the two is recorded in domain name servers throughout the Internet.

When Resolve Names is checked in the Log panel, VirusBarrier X6 will attempt to find the names for each of the Internet addresses shown in the log. If VirusBarrier X6 can find this information, it then displays it in name form rather than as numbers.

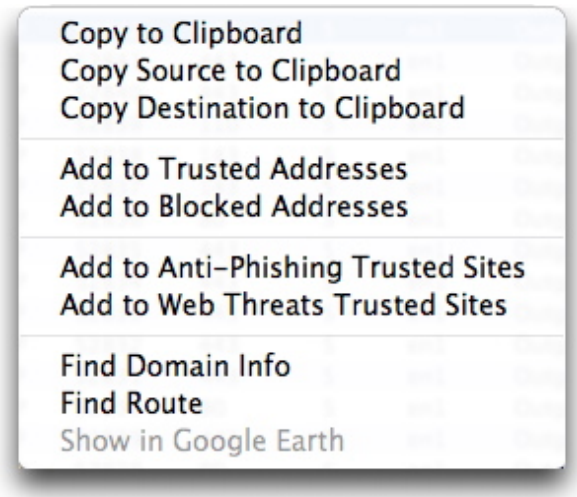


Date & Time	Source	Destination
1/11/11, 12:34:01 PM	192.168.1.19	www.intego.com
1/11/11, 12:33:57 PM	192.168.1.19	www.intego.com
1/11/11, 12:33:35 PM	192.168.1.19	www.intego.com
1/11/11, 12:33:16 PM	192.168.1.19	www.intego.com
1/11/11, 12:33:09 PM	192.168.1.19	www.intego.com

VirusBarrier X6 is not able to resolve the names of all Internet addresses, since some addresses have no name equivalents.

Network Log Window Contextual Menu

If you hold down the Control key and click any log entry, or right-click on a log entry, a contextual menu displays.



Its options are:

- **Copy to Clipboard**: Copies visible columns of this log entry to the Mac OS X clipboard, in tab-delimited text format. You can then paste it into any application or document.
- **Copy Source to Clipboard**: Copies only the Source field of this log entry to the Mac OS X clipboard: only available when viewing the log in Expert mode.
- **Copy Destination to Clipboard**: Copies only the Destination field of this log entry to the Mac OS X clipboard: only available when viewing the log in Expert mode.
- **Add to Trusted Addresses**: Permanently adds this IP address to the Trusted Addresses, thereby allowing future communications from it regardless of Antivandal settings. However, VirusBarrier X6's firewall will still affect communications from this IP address.
- **Add to Blocked Addresses**: Permanently adds this IP address to the Blocked Addresses, thereby preventing

future communications from it regardless of Antivandal settings.

- **Add to Anti-Phishing Trusted Sites**: Permanently adds this IP address to the list of Anti-Phishing Trusted Sites, thereby allowing future communications from it regardless of Anti-Phishing settings.
- **Add to Web Threats Trusted Sites**: Permanently adds this IP address to the list of Web Threats Trusted Sites, thereby allowing future communications from it regardless of Web Threats settings.
- **Find Domain Info**: Launches VirusBarrier X6's Whois window and performs a query on the selected IP address. See Whois Queries for more information.
- **Find Route**: Launches VirusBarrier X6's Traceroute window and performs a search on the selected IP address. See Traceroute Searches for more information.
- **Show in Google Earth**: Launches the Google Earth program, if you have it installed, and attempts to find the geographic location of the selected IP address.

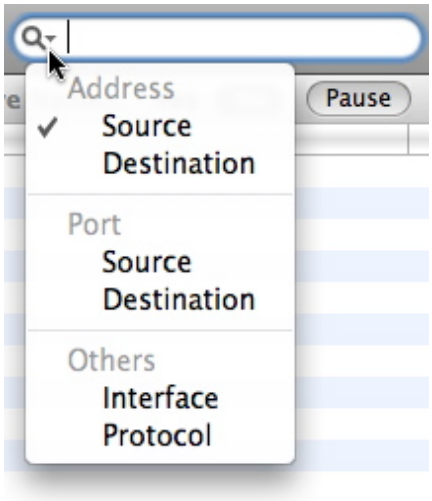
Filtering Data in the Network Log Window

At the top of the log window toolbar is a search field that lets you filter data according to several criteria, displaying only those entries that contain the selected criteria in the following categories:

- **Source address**
- **Destination address**
- **Source port**
- **Destination port**
- **Interface**
- **Protocol**

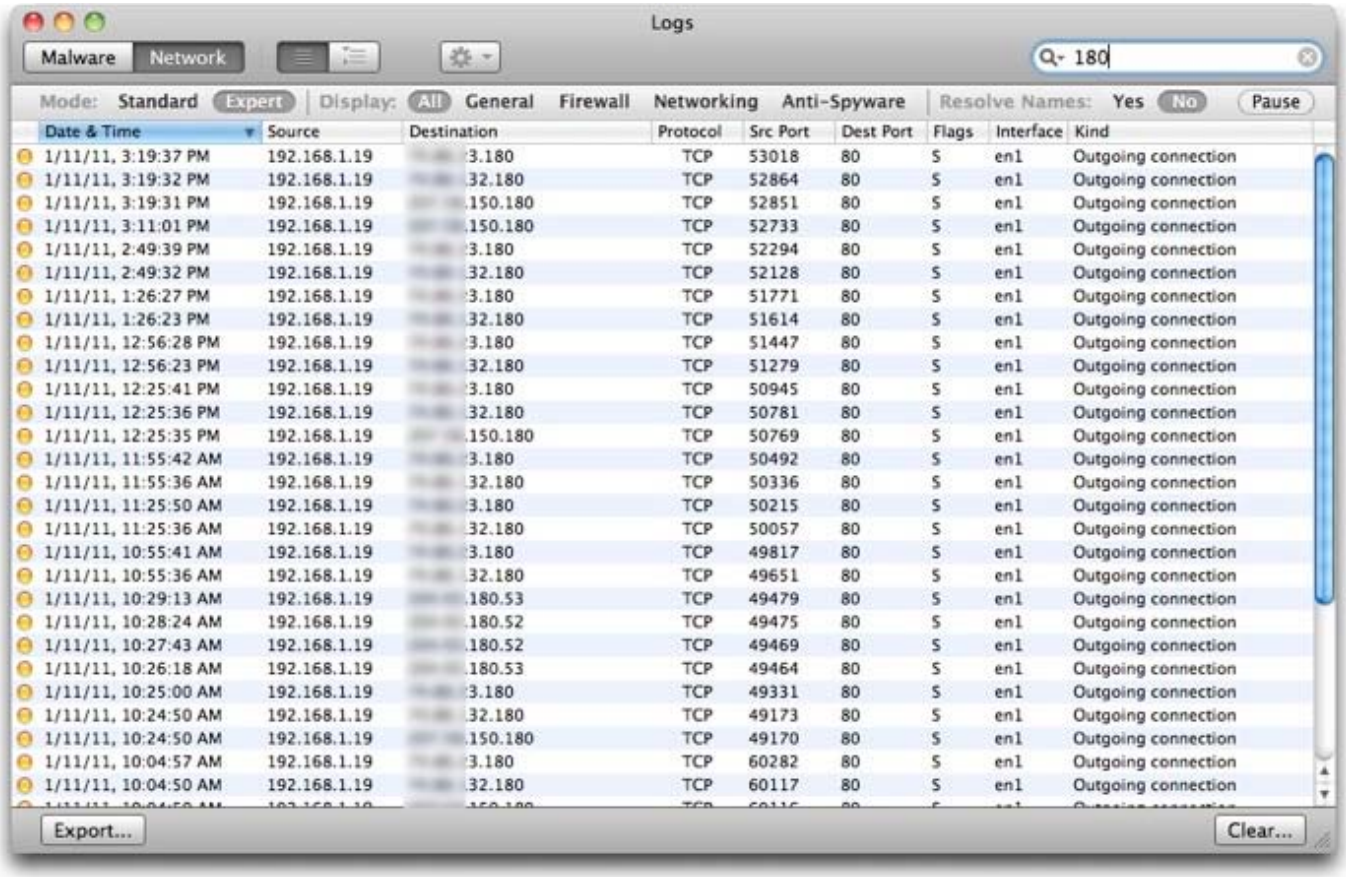
Source Address is the default criterion, as the search field shows.

To search for log data containing any of these criteria, click the disclosure triangle next to the Search icon.



Select the criterion you want to search for, then enter a string in the search field. You don't need to enter the entire string; the display is dynamic, and automatically narrows down log data as you enter characters in the search field.

In the example below, we're searching for "180" in the Destination Address. The search string can occur anywhere in the field, not just at the beginning. Also, the search works even if you're viewing the log in Standard mode, where the search field (the Destination, in this case) is hidden.



To clear the search field and begin a new search, click the small "X" button in the search field.

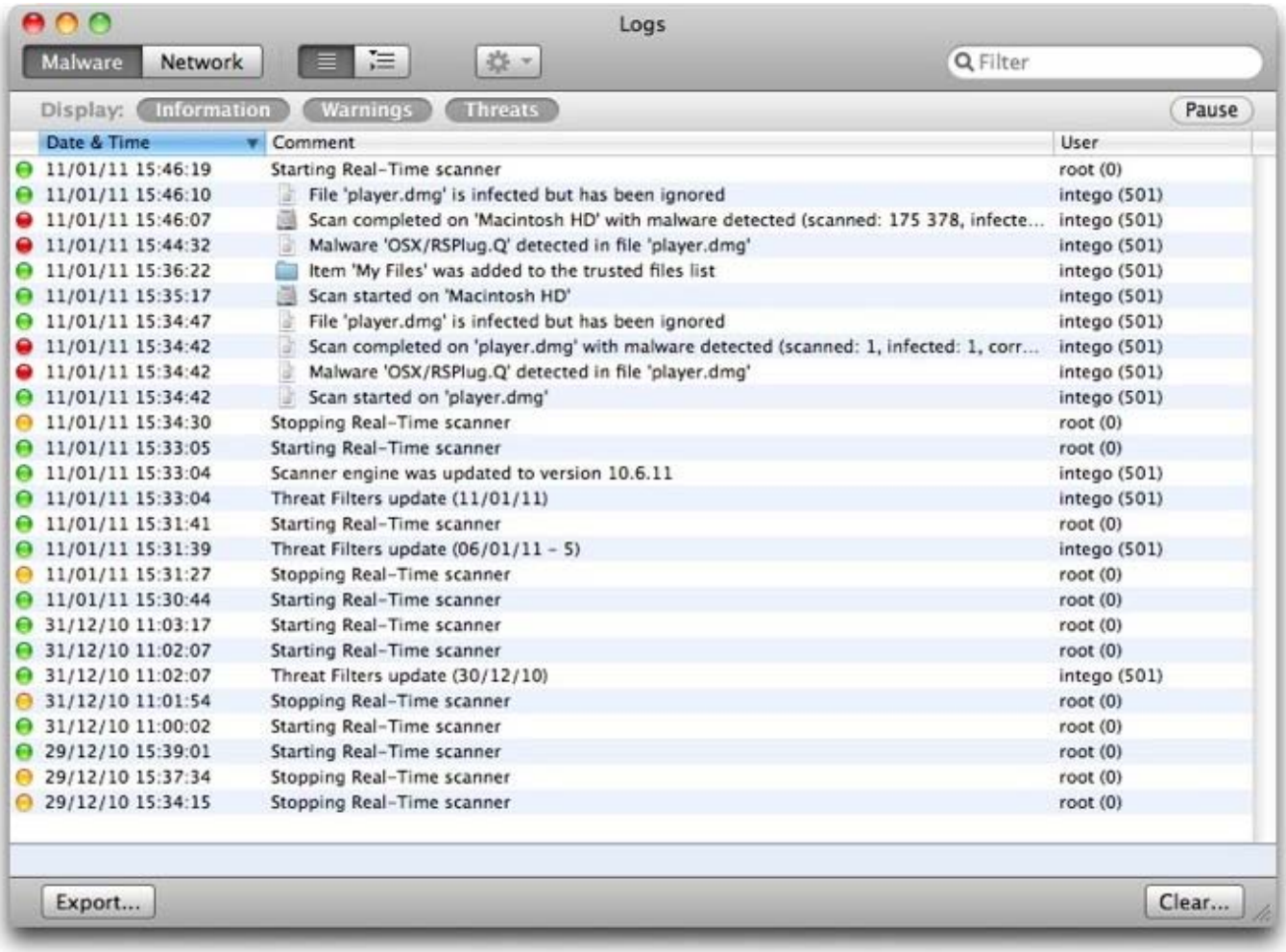
The Malware Log

The malware log shows a record of malware activity that VirusBarrier X6 has observed, including all manual and scheduled scans, and the results of these scans. As with the network log, you can filter it to highlight issues of interest.

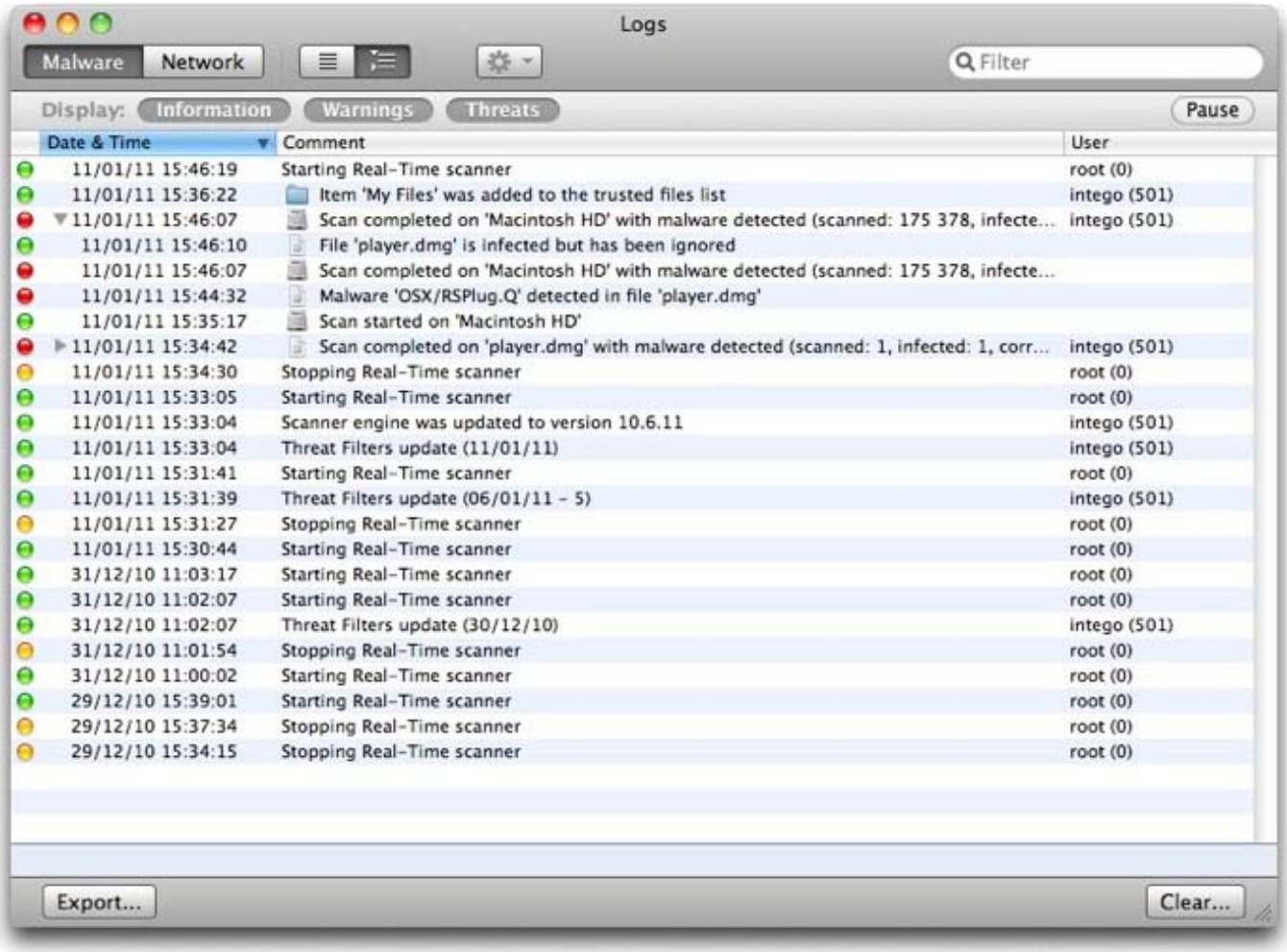
To access the malware log, click the small "magnifying glass" icon at the bottom of the screen, choose Window > Logs, or press Command-Option-L.

Then click the Malware button in the top-left corner if it isn't already selected.

The log looks as follows, although of course your log will show different entries from this one.


Logs
Malware
Network
Filter
Display:
Information
Warnings
Threats
Pause
Date & Time
Comment
User
11/01/11 15:46:19 Starting Real-Time scanner root (0)
11/01/11 15:46:10 File 'player.dmg' is infected but has been ignored intego (501)
11/01/11 15:46:07 Scan completed on 'Macintosh HD' with malware detected (scanned: 175 378, infecte... intego (501)
11/01/11 15:44:32 Malware 'OSX/RSPlug.Q' detected in file 'player.dmg' intego (501)
11/01/11 15:36:22 Item 'My Files' was added to the trusted files list intego (501)
11/01/11 15:35:17 Scan started on 'Macintosh HD' intego (501)
11/01/11 15:34:47 File 'player.dmg' is infected but has been ignored intego (501)
11/01/11 15:34:42 Scan completed on 'player.dmg' with malware detected (scanned: 1, infected: 1, corr... intego (501)
11/01/11 15:34:42 Malware 'OSX/RSPlug.Q' detected in file 'player.dmg' intego (501)
11/01/11 15:34:42 Scan started on 'player.dmg' intego (501)
11/01/11 15:34:30 Stopping Real-Time scanner root (0)
11/01/11 15:33:05 Starting Real-Time scanner root (0)
11/01/11 15:33:04 Scanner engine was updated to version 10.6.11 intego (501)
11/01/11 15:33:04 Threat Filters update (11/01/11) intego (501)
11/01/11 15:31:41 Starting Real-Time scanner root (0)
11/01/11 15:31:39 Threat Filters update (06/01/11 - 5) intego (501)
11/01/11 15:31:27 Stopping Real-Time scanner root (0)
11/01/11 15:30:44 Starting Real-Time scanner root (0)
31/12/10 11:03:17 Starting Real-Time scanner root (0)
31/12/10 11:02:07 Starting Real-Time scanner root (0)
31/12/10 11:02:07 Threat Filters update (30/12/10) intego (501)
31/12/10 11:01:54 Stopping Real-Time scanner root (0)
31/12/10 11:00:02 Starting Real-Time scanner root (0)
29/12/10 15:39:01 Starting Real-Time scanner root (0)
29/12/10 15:37:34 Stopping Real-Time scanner root (0)
29/12/10 15:34:15 Stopping Real-Time scanner root (0)
Export...
Clear...

There are two ways you can display log information. In the example above, log entries are shown in linear order, each one taking up one line. You can click the second button at the top-left of the window and display log entries in hierarchical order, where disclosure triangles group related entries:

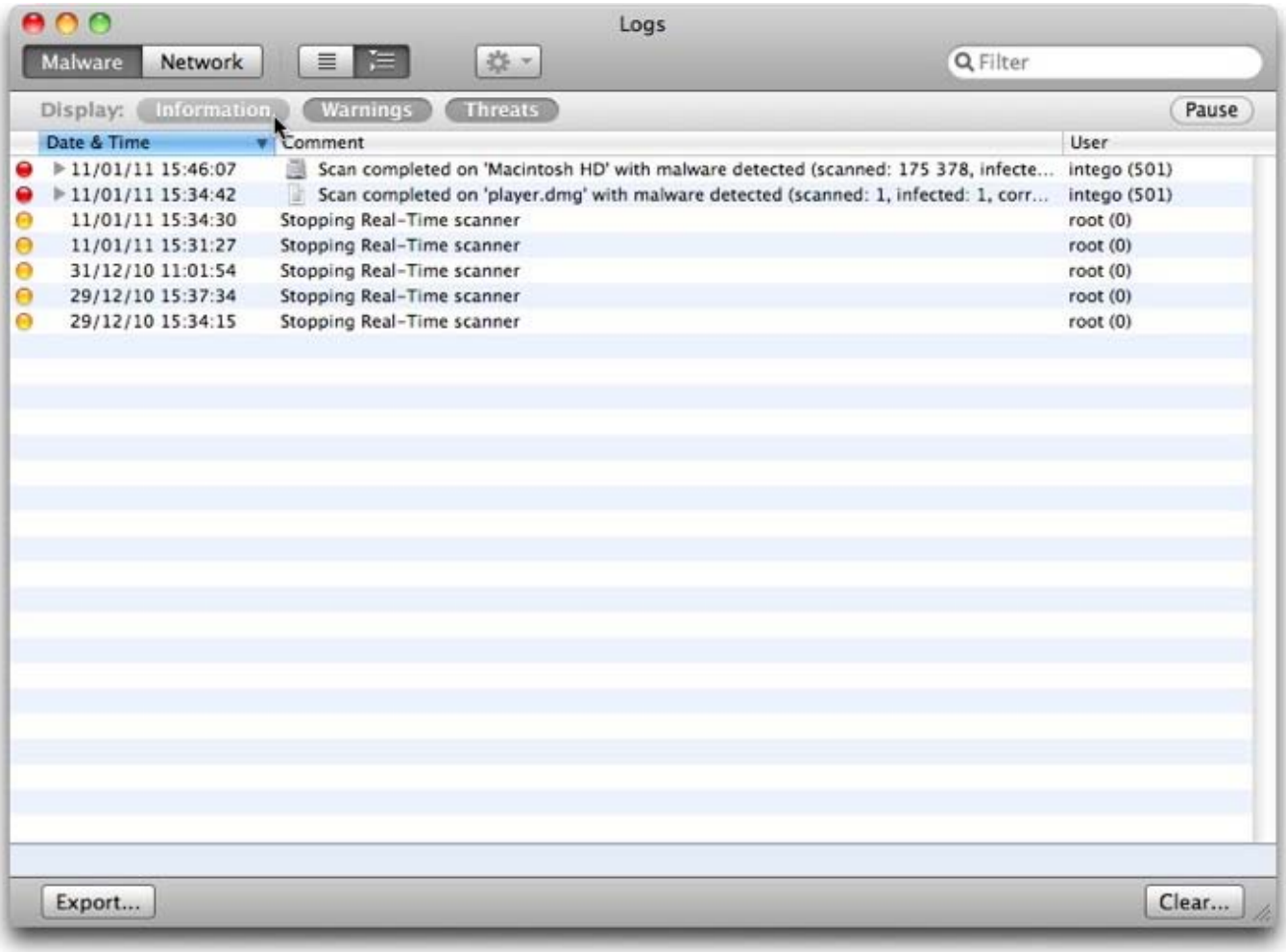

Logs
Malware
Network
Filter
Display:
Information
Warnings
Threats
Pause
Date & Time
Comment
User
11/01/11 15:46:19 Starting Real-Time scanner root (0)
11/01/11 15:36:22 Item 'My Files' was added to the trusted files list intego (501)
11/01/11 15:46:07 Scan completed on 'Macintosh HD' with malware detected (scanned: 175 378, infecte... intego (501)
11/01/11 15:46:10 File 'player.dmg' is infected but has been ignored
11/01/11 15:46:07 Scan completed on 'Macintosh HD' with malware detected (scanned: 175 378, infecte...
11/01/11 15:44:32 Malware 'OSX/RSPlug.Q' detected in file 'player.dmg'
11/01/11 15:35:17 Scan started on 'Macintosh HD'
11/01/11 15:34:42 Scan completed on 'player.dmg' with malware detected (scanned: 1, infected: 1, corr... intego (501)
11/01/11 15:34:30 Stopping Real-Time scanner root (0)
11/01/11 15:33:05 Starting Real-Time scanner root (0)
11/01/11 15:33:04 Scanner engine was updated to version 10.6.11 intego (501)
11/01/11 15:33:04 Threat Filters update (11/01/11) intego (501)
11/01/11 15:31:41 Starting Real-Time scanner root (0)
11/01/11 15:31:39 Threat Filters update (06/01/11 - 5) intego (501)
11/01/11 15:31:27 Stopping Real-Time scanner root (0)
11/01/11 15:30:44 Starting Real-Time scanner root (0)
31/12/10 11:03:17 Starting Real-Time scanner root (0)
31/12/10 11:02:07 Starting Real-Time scanner root (0)
31/12/10 11:02:07 Threat Filters update (30/12/10) intego (501)
31/12/10 11:01:54 Stopping Real-Time scanner root (0)
31/12/10 11:00:02 Starting Real-Time scanner root (0)
29/12/10 15:39:01 Starting Real-Time scanner root (0)
29/12/10 15:37:34 Stopping Real-Time scanner root (0)
29/12/10 15:34:15 Stopping Real-Time scanner root (0)
Export...
Clear...

The Log shows every time that:

- You start a scan
- You cancel a scan in mid-process
- You start or stop the real-time scanner
- VirusBarrier X6 finishes a scan, with its results
- VirusBarrier X6 discovers a virus
- VirusBarrier X6 discovers a corrupted file
- VirusBarrier X6 repairs an infected file
- Files are added to or removed from the Quarantine Zone
- Files are added to or removed from the Trusted Files list
- Virus definitions are updated

The colored dots in the leftmost column show you what types of entries are displayed in the log. Green dots indicate information, such as starting the real-time scanner or updating virus definitions. Orange dots are for warnings, such as stopping the real-time scanner. Red dots indicate threats, such as when infected or corrupted files are found. The files, folders or volumes selected for each scan are named, as are all problems found.

You can choose to only display certain types of information by clicking one of the three log type buttons to hide or display their entries.



You can perform actions on some log entries by selecting them and clicking on the Action button in the log window toolbar, or by Control-clicking or right-clicking. You'll see a contextual menu that offers three options:

- **Show in Finder**: this opens a Finder window with the selected file highlighted so you can see where it is and either delete it or perform other actions on it.
- **Delete from Disk**: this option is only available for corrupted files; if you choose it, the corrupted file will be deleted from your disk
- **Submit Suspicious File to Intego**: choose this to send any suspicious files to Intego for our Virus Monitoring Center to examine

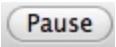
You can also filter search results by entering text in the search field in the window's toolbar. As you type text, the results will narrow down, showing only those log entries that contain the text you have typed.

You can copy any log items by selecting them and pressing Command-C; you can then paste them into another application, if needed.

You can remove any log items by selecting them and pressing Delete. You can clear the entire log by clicking the **Clear...** button.

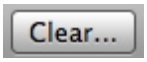
Features Common to Both the Network and Malware Logs

Pausing the Log



If you have many connections entering and leaving your computer, you may find it difficult to follow the log as it displays. To view the log more easily, click the **Pause** button in the log window's upper-right corner. The log display stops so you can read the data, but keeps recording and will display new data when the log is no longer paused. Click the **Pause** button again to resume real-time display.

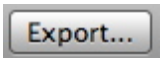
Clearing the Log



To clear the log, and erase all information it contains, click the **Clear...** button in the lower-right corner. A dialog appears, asking you to confirm your request.

The log will also be cleared automatically if you've checked the **Clear log after exporting** checkbox in the Log Preferences and have set VirusBarrier X6 to export a log periodically. See Preferences and Configurations for more about log preferences.

Exporting the Log



You can export log data in several formats. When doing a manual export, only the data displayed is exported. If you have only checked, say, **Firewall** in the Log panel, only firewall data will be exported. (You can also have the Log data exported automatically: See Preferences and Configurations for more about log preferences.)

To export Log data, click the **Export...** button. A dialog will prompt you to save the file; you may change its name if you wish. Choose where you wish to save it; by default, export files are saved to your Documents folder.

WARNING: Log exports may take several minutes if the Resolve Names feature is turned on.

Logs can be exported in six formats. Click the **Format** popup menu to select the export format.

The available formats are:

- **Expert HTML**: HTML format, showing all columns visible in Expert mode. In this format you can partially retrace past browsing history, as VirusBarrier X6 provides clickable links for all log entries for non-secure Web pages. (That is, Destination Ports, connected by TCP, targeting ports 80 or 8080.)
- **Expert Text**: Tab-delimited, plain text format with additional columns to show all columns visible in Expert mode. This is the best mode to use for import into a spreadsheet or database program.
- **HTML**: HTML format, showing all columns visible in Standard mode. As with Expert HTML exports, this file

format helps you retrace past browsing history.

- **Analytic**: A text format similar to Expert Text, without tab separators, but with labels in front of some fields.
- **Text**: Tab-delimited, plain text format with all columns visible in Standard mode.
- **Who's there?**: The log as a text file, with the following columns: Date, Time, Result, Hostname, Server Port, and Method: useful in some log analysis programs.

Traffic Monitors

VirusBarrier X6 has a number of tools that let you monitor network traffic entering or leaving your Mac, conduct queries and searches on network addresses and see which services and networks are available to your Mac.

Traffic Window

The Traffic window contains a set of activity gauges that tell you the type and quantity of network activity that is coming into and going out of your Mac from both the Internet and local networks. To access the Traffic window, click the small icon shown below, choose **Window** > **Traffic**, or press Command-Option-4.

The Traffic screen has four viewing modes, switchable by clicking the small buttons at the top of the screen.

The first button is the default view and shows traffic as two rows of gauges and a timeline.

The IN gauges on top, with values shown in orange by default, display the amount of data coming into your Mac. The OUT gauges in the second row, with values shown in green by default, display the amount of data leaving your computer. The number inside the gauge is the current throughput in kilobytes per second (k/s), and the bottom is the total amount, usually in megabytes (MB) or gigabytes (GB).

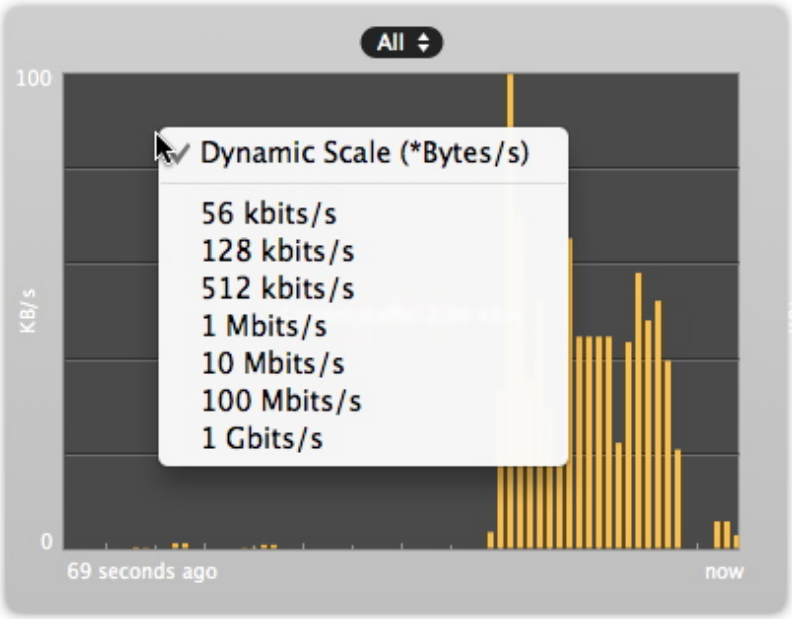
The timeline at the bottom shows traffic over time, where the bars the furthest to the right represent the present time, and those to the left represent the past. As above, orange values show incoming traffic while green values show outgoing traffic.

By default, the timeline records activity going back 111 seconds in time. You can increase this time period by making the window larger, either by clicking the green zoom button in the upper-left corner, or by clicking and dragging the window's bottom-right corner. The maximum time is determined by the size of your screen or your willingness to see only a section of the timeline at one time.

If you place your cursor over a timeline, text appears showing the current average data throughput, which is updated every second.

The second view button shows traffic as three timelines, respectively showing traffic in, out, and in total.

This view mode has a special feature that lets you choose the scale for the In and Out graphs by moving the mouse over one of them, holding down the Control key, and clicking, or right-clicking, a popup menu offers several options.



This lets you choose your maximal throughput and displays graphs that are correctly scaled for that throughput. Choose **Dynamic Scale** if you want the graph to change its scale according to the data throughput as described earlier.

The third view mode button shows traffic as a series of gauges in horizontal orientation, with no timeline. The fourth button shows the same gauges, but in a vertical orientation (not shown here).

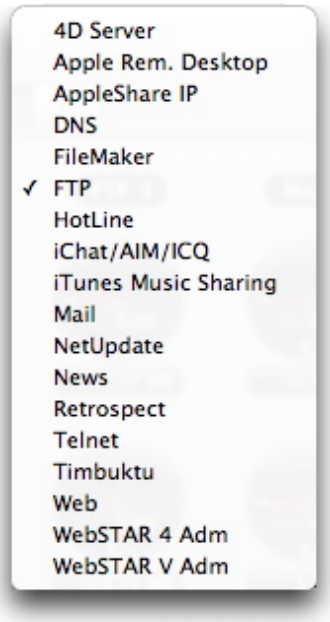
The three views that contain round gauges also have Reset buttons. Clicking this button sets the totalizing, bottom row of gauges back to zero.

Selecting Activity Data Types

In each view mode, you have a choice of which type of traffic to view: by default, the activity data types monitored are Web, FTP, Mail, iChat/AIM. The fifth gauge shows all other traffic, while the sixth shows total traffic.

But you can choose which type of data will be shown for the first four pairs of gauges by clicking the indicator over one of the gauges.

A popup menu displays showing several choices.



You can add or remove services from this list through the Traffic Preferences pane: see Traffic Preferences in See Preferences and Configurations for details.

Viewing Network Traffic in the Menu Bar

VirusBarrier X6 can also display network traffic in the menu bar. You can access this feature from VirusBarrier X6's Preferences. Choose **VirusBarrier X6** > **Preferences...** then click on the **Traffic** icon. Check **Display network traffic in the menu bar** to turn this feature on. This displays the amount of incoming and outgoing traffic at all times. You can turn this off by unchecking **Display network traffic in the menu bar**.

VirusBarrier Traffic Monitor

Installing VirusBarrier X6 also places an application called VirusBarrier Traffic Monitor in your Applications folder. You can launch this program by double-clicking its icon, or from the Intego Menu by choosing **VirusBarrier X6** > **Open VirusBarrier Traffic Monitor**.

VirusBarrier Traffic Monitor

The VirusBarrier Traffic Monitor application provides a small, floating window that lets you keep an eye on network activity at all times, without needing to display the entire VirusBarrier X6 activity gauge palette.

When you open VirusBarrier Traffic Monitor, it displays its activity gauge window in the bottom-right corner of your screen. You can move VirusBarrier Traffic Monitor by clicking it and dragging to a new place on your screen.

By default, VirusBarrier Traffic Monitor displays the total network traffic for all services. You can change what kind of traffic is displayed by clicking All at the bottom of the VirusBarrier Traffic Monitor window, and selecting a service from the popup menu.

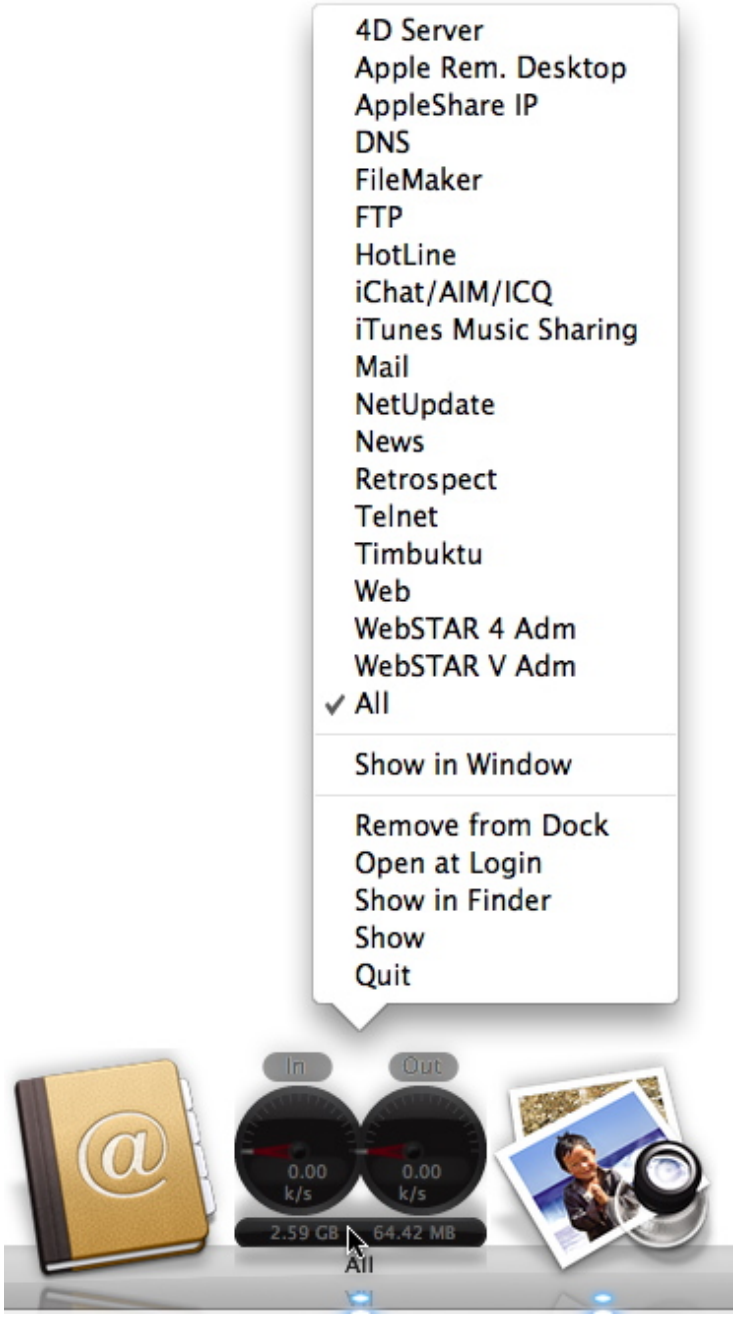
If you hold down the Control key on your keyboard and click anywhere in the VirusBarrier Traffic Monitor window, a popup menu offers two options.

Show in Dock closes VirusBarrier Traffic Monitor's window, and the program's Dock icon changes to show its activity gauges, updated in real time.

Network activity also appears in the VirusBarrier Traffic Monitor icon you see when you switch among applications by pressing Command-Tab.

To return VirusBarrier Traffic Monitor to its window, hold down the Control key, click on the VirusBarrier Traffic Monitor Dock icon, and select **Show in Window**.

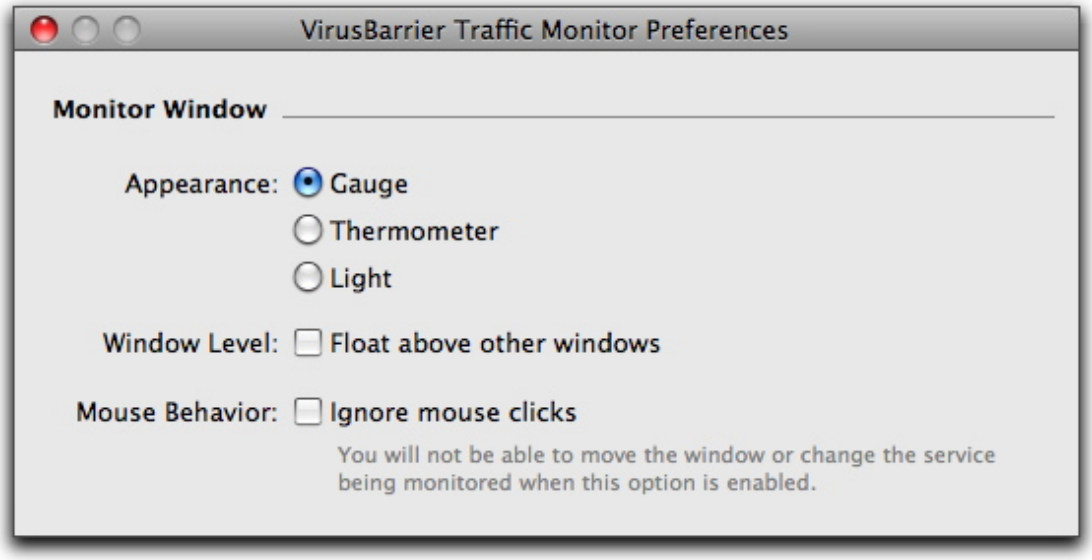
When VirusBarrier Traffic Monitor displays in the Dock, you can change its display by holding down the Control key, clicking on its Dock icon, and selecting a different service from its Dock menu.



The **Keep in Dock** selection makes the VirusBarrier Traffic Monitor icon a permanent fixture in the Dock, even when the program is not running, so you can open it just by clicking its Dock icon. The Open at Login selection starts the program each time you start a user's session on your Mac.

VirusBarrier Traffic Monitor Preferences

Several preference settings affect the behavior of VirusBarrier Traffic Monitor. To set them, go to **VirusBarrier Traffic Monitor** > **Preferences** or press Command-comma while VirusBarrier Traffic Monitor is running.



- **Appearance**: Choose from **Gauge**, **Thermometer** or **Light**:

- **Window Level**: **Float above other windows** makes VirusBarrier Traffic Monitor always appear in the foreground, above all other applications.
- **Mouse Behavior**: **Ignore mouse clicks** prevents you from moving VirusBarrier Traffic Monitor's window or changing the service it monitors.

The VirusBarrier Traffic Monitor Widget

VirusBarrier X6 installs the VirusBarrier Traffic Monitor widget that loads into Mac OS X's Dashboard to show you network activity when you are in Dashboard.

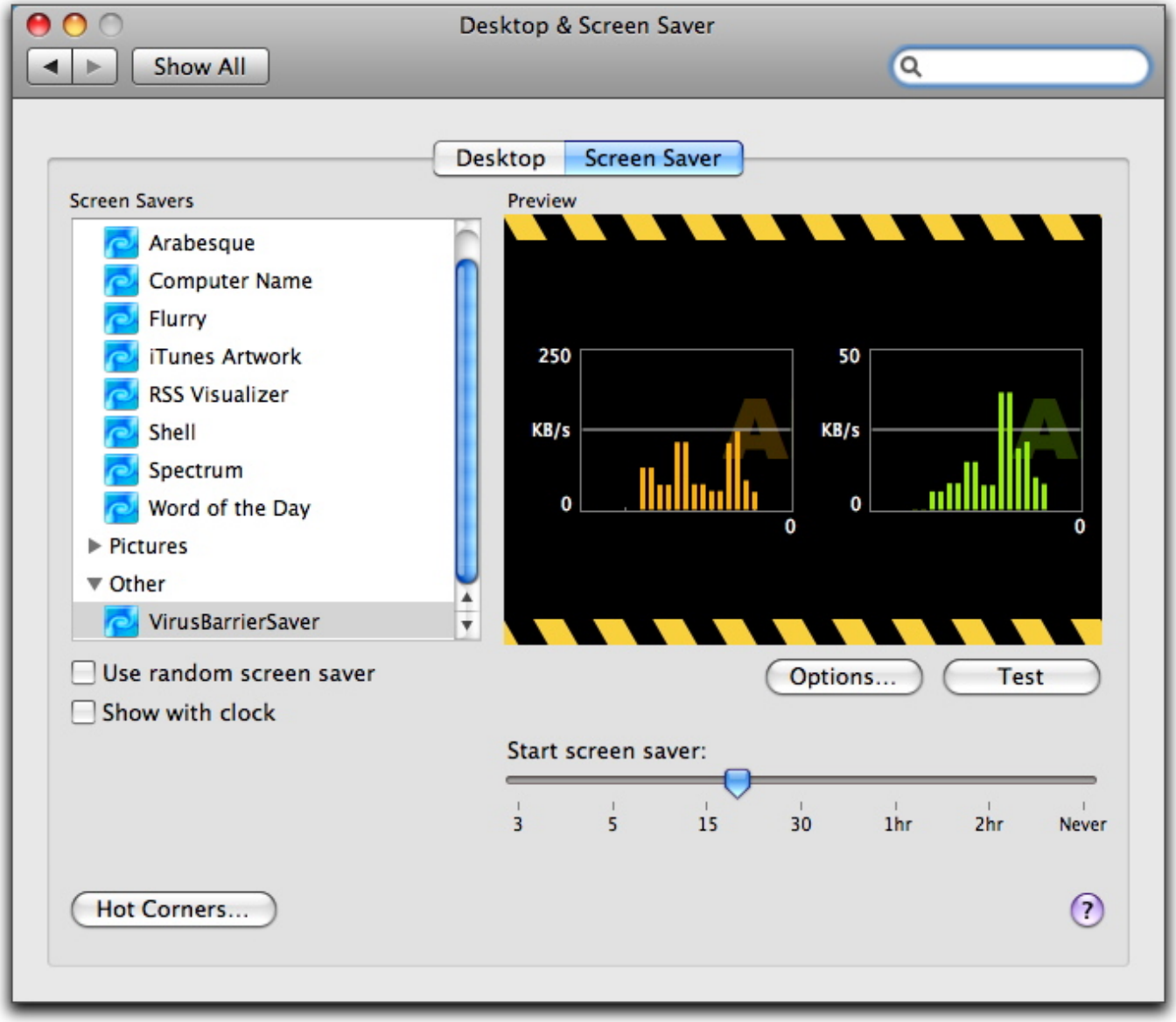
To display the VirusBarrier Traffic Monitor widget, activate Dashboard. Click the + button to display all the widgets available on your computer. Select VirusBarrier Traffic Monitor from the list. Its icon looks like this:

If you add it to your active widgets, you will see VirusBarrier Traffic Monitor whenever you switch to Dashboard. As with the VirusBarrier Traffic Monitor application, you can move the window or change the type of activity displayed.

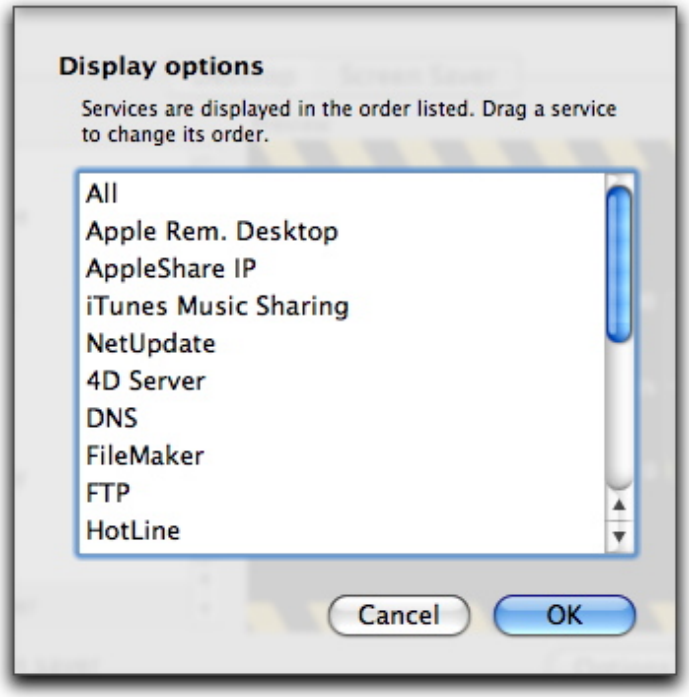
The VirusBarrier X6 Monitor Screen Saver

VirusBarrier X6 installs a screen saver that gives you an overview of network activity when your computer is otherwise idle. In addition, if your Macintosh is running as a server, you can use this screen saver to keep an eye on its network activity.

To use the VirusBarrier X6 screen saver, open the System Preferences from the Apple menu, click on **Desktop & Screen Saver**, and click the **Screen Saver** tab. Select **VirusBarrierSaver** in the screen saver list.



The preview screen only shows All traffic; however, it will show traffic broken down by service when actually running. Click on **Options** to choose the order in which services are displayed.



Drag them into the order you want. The number of services displayed depends on your screen resolution and the number of screens you have: therefore, the ones most important to you should be listed first.

For more on screen saver settings, see the Mac OS X help.

Viewing Active Services

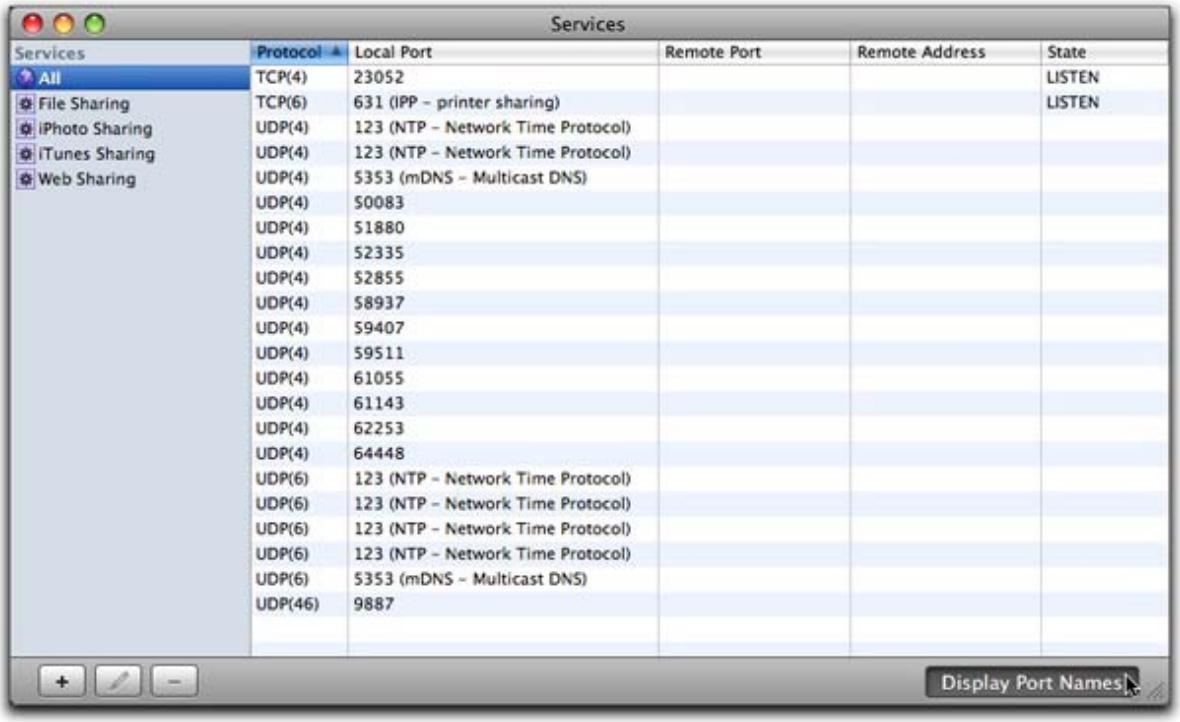
VirusBarrier X6's Services window lists all active network services on your computer that are accessible to other users via Internet Protocol, such as a web server, mail server, etc.

To show the Services window, click the double-arrow icon in the bottom-right corner of VirusBarrier X6's main window.

For each port used you see the following information:

- The protocol (TCP or UDP)
- The local port number (depending on the protocol it represents, if it is a standard protocol, such as port 21 for FTP)
- The remote port number
- The remote address (the IP address of the remote connection)
- The state of the connection - for example, whether the connection is active or if it's just listening for traffic.

To obtain the names of the ports in addition to their numbers, click the **Display Port Names** button in the lower-right corner, as is shown here.

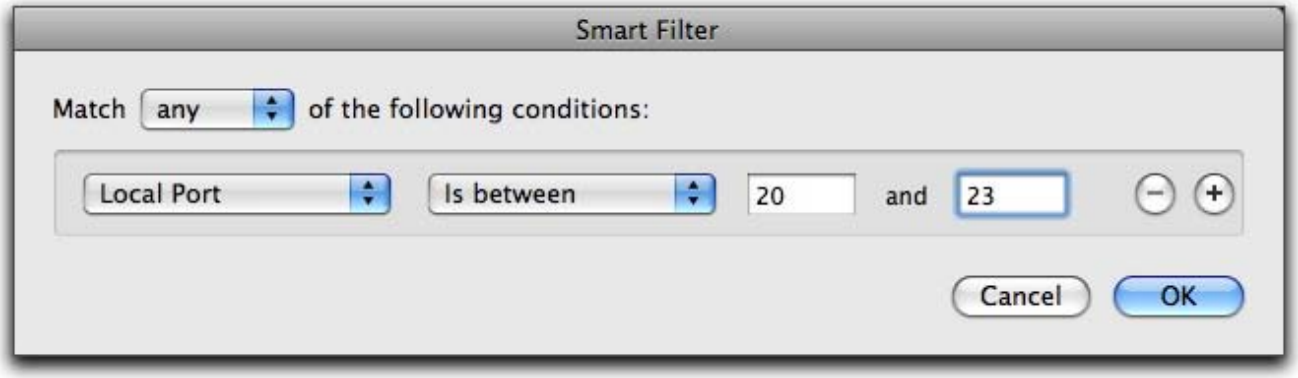


Since the list of ports used by all services can be long, VirusBarrier X6 provides filters to allow you to view ports used by specific services. You can choose from **File Sharing**, **iPhoto Sharing**, **iTunes Sharing** and **Web Sharing** by clicking in the left column, or you can create your own filters.

To create a filter, click the + button in the lower-left corner of the panel. The **Smart Filter** window displays.

The first popup menu lets you specify whether you want the filter to match **Any** of the conditions you give, or **All** of them.

The second popup menu specifies the type of information that you want the filter to find. The choices are the same as the Services window's columns: **Protocol**, **Local Port**, **Remote Port**, **Remote Address** and **State**. After choosing one of these, you'll have the opportunity to specify filter details. In this example, we're only going to list those services where the local port is in a given range.



Clicking the + button at the right of the window adds additional conditions, while clicking the - button next to a condition removes it from the list. You can also modify filter conditions by simply changing their popup menu options or typing new data into the data fields.

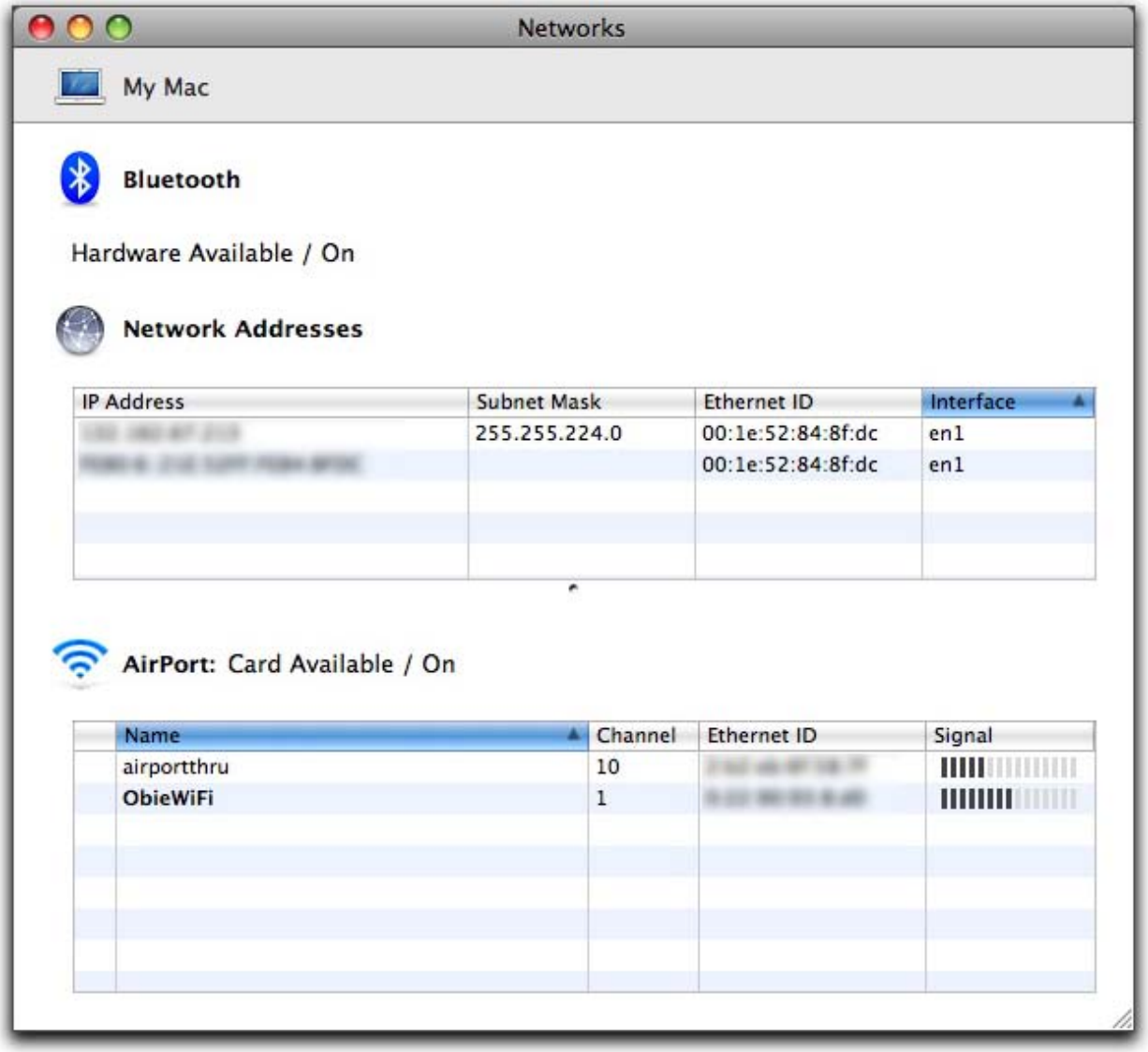
When you finish creating your filter, click OK to save it, then enter a name for the filter in the **Services** list. Click the filter at any time in the list to view the network services that correspond to your conditions.

Viewing Network Information

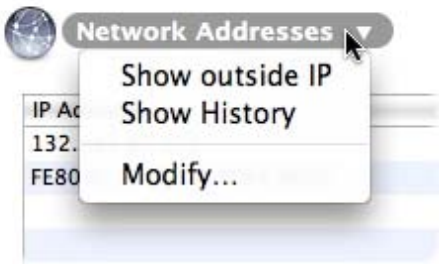
The Networks window provides useful information about your Mac, its network configuration, and local networks available to it. To show the Networks window, click the radio icon in the bottom-right corner of VirusBarrier X6's main window.

The Networks window shows:

- **Your Mac's name**: Shown in the gray bar at top: in the example below, it's "My Mac". This is the name that your computer shows to anyone browsing for it on a network. You can change this name in the Sharing pane of the System Preferences.
- **Bluetooth**: Whether Bluetooth hardware is available and active.
- **Network Addresses**: All the IP addresses that are active on your Mac. If you have several network adapters with different addresses, or are running several servers, more than one address will be shown. It also tells you about any related Subnet Masks, Ethernet IDs and Interfaces (in BSD name format).
- **AirPort**: Availability and status of a wireless networking card. If your AirPort card is available and on, the table shows available wireless networks, their Channels, Ethernet IDs, and signal strengths in relation to your current position. (The more dark bars, the stronger the signal.) Wireless networks that require a password or other key to join display a small icon of a lock. Those with no lock have no networking password: however, they may be protected in other ways, such as via Web authentication. If you're connected to a wireless network, its name will appear in bold type.



Several functions and options are available for the Networks screen by clicking on the words **Network Addresses**.



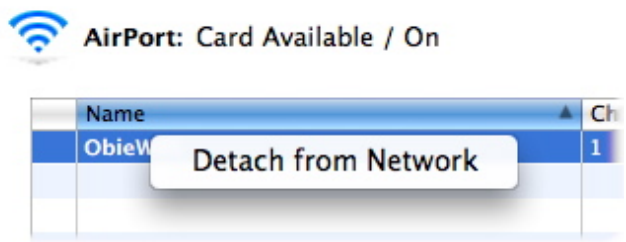
These options are:

- **Show outside IP**: Shows in large type the IP address that your computer uses when it connects to the Internet or other networks. This address is different from what VirusBarrier X6 displays on this pane if you have a router, a cable or a DSL modem. Click anywhere on the screen to dismiss the information.
- **Show History**: Displays a list showing the different IP addresses attributed to your Mac by your ISP, if you have dynamic IP addressing. However, if you have a router, or a cable modem, this only shows the IP address your computer uses internally.
- **Modify...**: Opens the Network pane of Mac OS X's System Preferences. You can change your computer's network settings in this pane. For more on Network settings, see the Mac OS X help.

Additional options are available for individual entries in the **Network Addresses** area as well. To reveal them, press the Control key while clicking on the entry you mean to affect. A contextual menu appears.

- **Copy IP Address to Clipboard**: Puts the information in plain text form on the Mac OS X clipboard, where you can paste it in other applications.
- **Large Type**: Offers to show a full-screen display of any of three kinds of information related to the entry: its **IP address**, **Subnet Mask** or **Ethernet ID**. Clicking anywhere on the screen dismisses the large-type display.

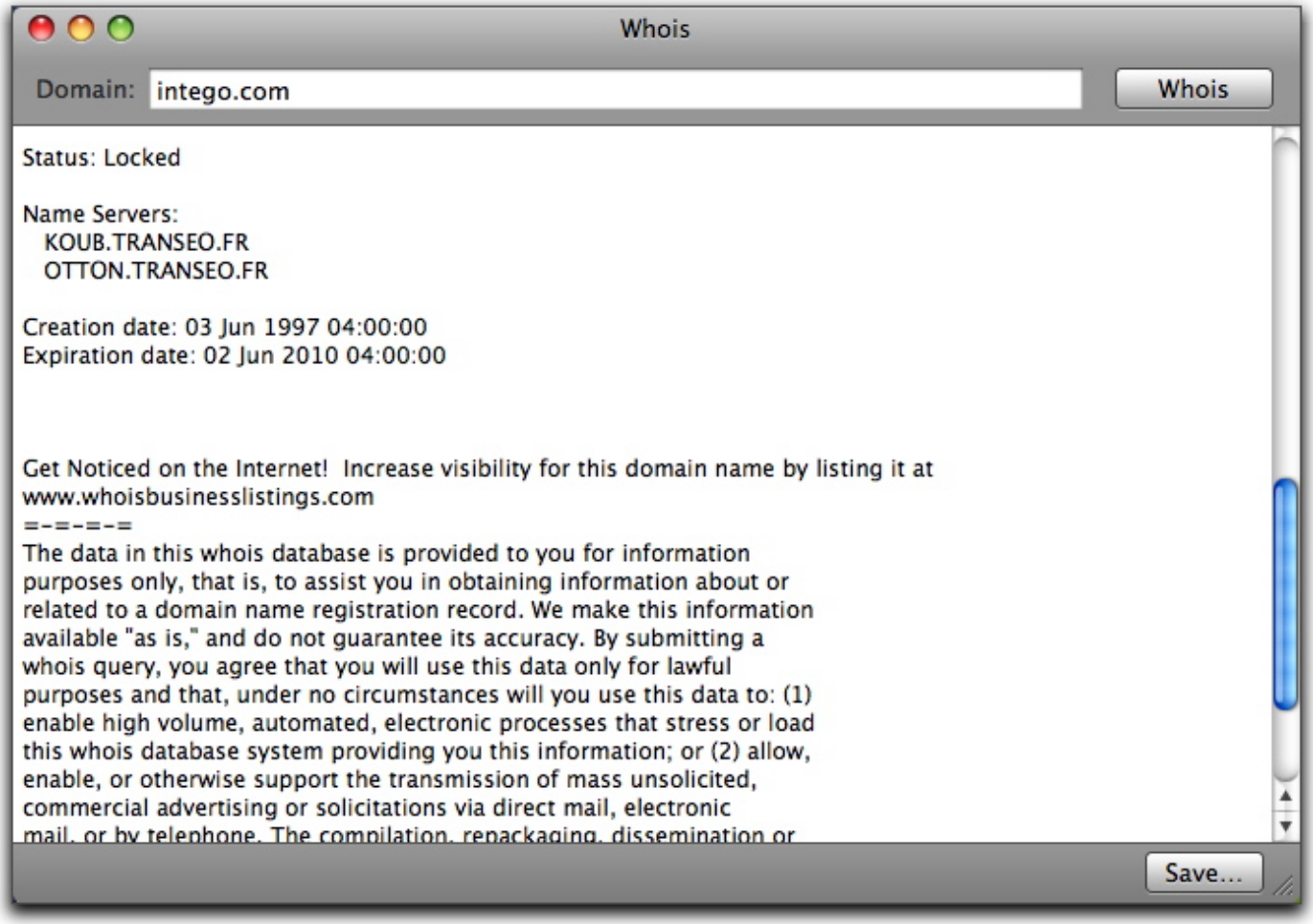
Finally, Control-clicking on entries in the AirPort section brings up a contextual menu where you can detach your Mac from a network to which you're currently attached.



Whois Queries

VirusBarrier X6 allows you to look up domain names and Internet IP addresses using its built-in Whois tool, which you launch by clicking the "?" button in the bottom-right corner of the screen.

Then, enter a domain name or IP address in the **Domain** field, and click the **Whois** button or press the Enter key. The large text field below gives you information about the domain, fetched from publicly accessible information servers. You can save this information to a text file by clicking the **Save...** button.


Whois
Domain:
intego.com
Whois
Status: Locked
Name Servers:
KOUB.TRANSEO.FR
OTTON.TRANSEO.FR
Creation date: 03 Jun 1997 04:00:00
Expiration date: 02 Jun 2010 04:00:00
Get Noticed on the Internet! Increase visibility for this domain name by listing it at
www.whoisbusinesslistings.com
=-=-=-=
The data in this whois database is provided to you for information
purposes only, that is, to assist you in obtaining information about or
related to a domain name registration record. We make this information
available "as is," and do not guarantee its accuracy. By submitting a
whois query, you agree that you will use this data only for lawful
purposes and that, under no circumstances will you use this data to: (1)
enable high volume, automated, electronic processes that stress or load
this whois database system providing you this information; or (2) allow,
enable, or otherwise support the transmission of mass unsolicited,
commercial advertising or solicitations via direct mail, electronic
Save...

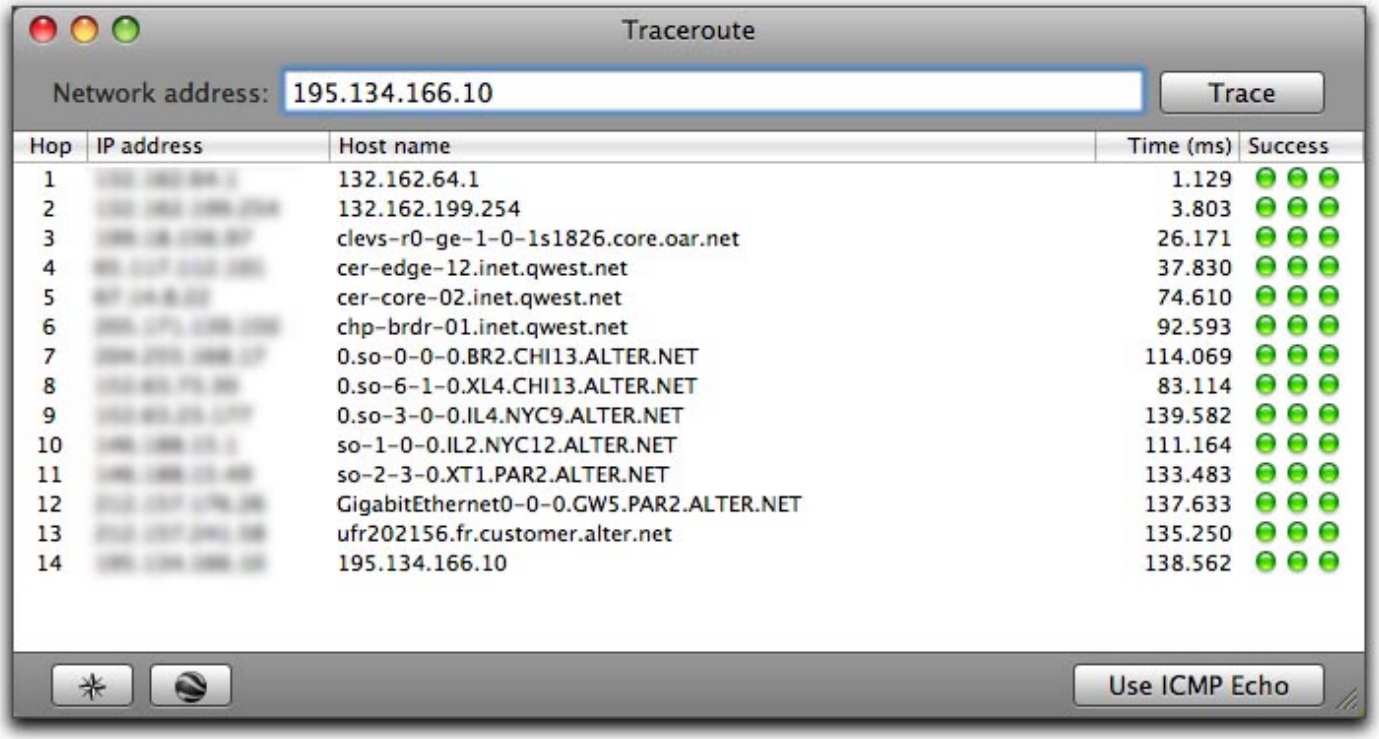
After you receive your information, text in the gray bar at the bottom of the window tells you the name of the server where that information originated. VirusBarrier X6 includes four default Whois servers, but you can change these or add others. To find out how to add Whois servers, see See Preferences and Configurations.

Traceroute Searches

When you send or receive data over the Internet or other networks, it travels in packets from host to host until it reaches its destination, possibly making dozens of hops along the way. VirusBarrier X6's traceroute function can help you see exactly how your data gets to its destination; this is especially useful when you are having problems accessing a specific host, and want to see where the data is blocked. When this happens, it usually means a key host or router is not functioning.

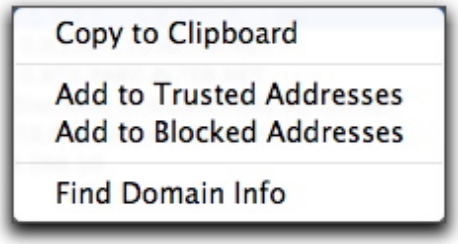
Launch VirusBarrier X6's traceroute tool by clicking the "Y-arrow" button in the bottom-right corner of the screen.

To run a traceroute search, enter an IP address or a domain name in the **Network** address field, then click Trace or press the Return key. If you enter a domain name, VirusBarrier X6 resolves it and displays the actual IP address. If you click **Use ICMP Echo**, the traceroute sends ICMP requests instead of UDP requests; in some cases, this may be more effective.



The Traceroute window then shows all the hops between your computer and the final host. For each hop, VirusBarrier X6 displays the hop number, the IP address, the host name, the response time in milliseconds, and the number of pings that succeed (green circles) or fail (red circles). VirusBarrier X6 sends three pings for each hop, or each step along the route. Note that if you have a router on your network, it may not respond to the traceroute request, and may display as failed requests. This won't prevent the rest of the traceroute from being executed.

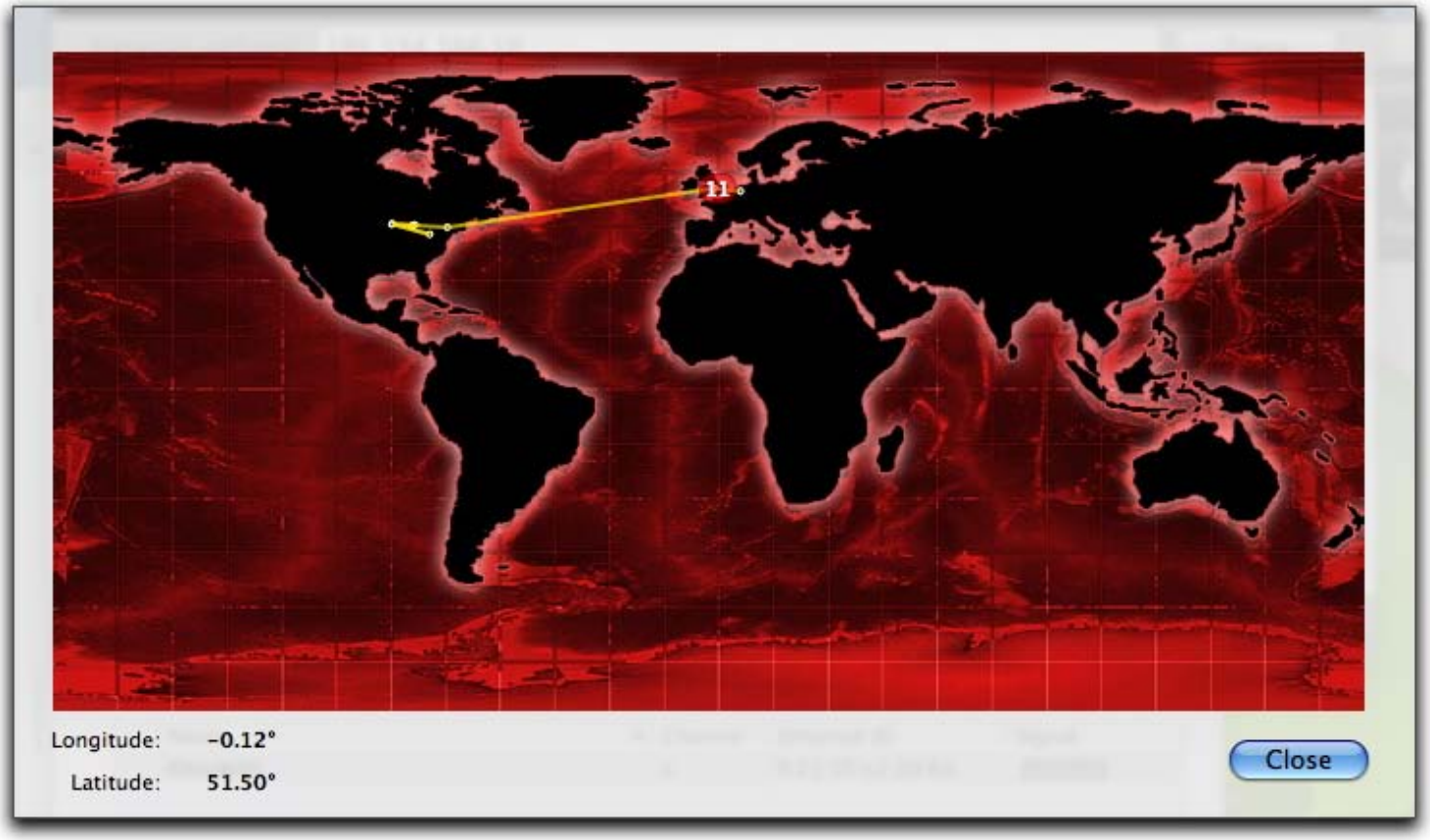
After your traceroute search has completed, you can Control-click on an entry to view a contextual menu.



- **Copy to Clipboard**: Puts the information in plain text form on the Mac OS X clipboard, so you can paste it in other applications.
- **Add to Trusted Addresses**: Permanently adds this IP address to the Trusted Addresses list, thereby allowing future communications from it regardless of Antivandal settings. However, VirusBarrier X6's firewall will still affect communications from this IP address.
- **Add to Blocked Addresses**: Permanently adds this IP address to the Blocked Addresses list, thereby blocking future communications from it regardless of Antivandal settings.
- **Find Domain Info**: Launches VirusBarrier X6's Whois window and performs a search on the selected IP address.

You can see a visual display of the route your data takes by clicking the map rosette button in the bottom-left corner.

This shows a world map with lines connecting each hop, and numbers showing their position on the path.



If you click the Google Earth button in the bottom-left corner, and you have Google Earth software installed on your Mac, VirusBarrier X6 will open Google Earth and zoom to the precise geographical location of the IP address.

Note that this will not work with addresses on your local network, and it will not work with all IP addresses.

‹‹ Protecting Your Mac from Network Attacks

VirusBarrier X6 Preferences and Configurations ››

© 2011 Intego. All Rights Reserved.

VirusBarrier X6 Preferences and Configurations

- General Preferences
- Modem Preferences
- Log Preferences
- Traffic Preferences
- Whois Preferences
- Advanced Preferences
- Working with Configurations

Go to Main Table of Contents

VirusBarrier X6 is designed to work unobtrusively in the background once it's installed. However, it has numerous options to let you control how its various functions run, and how you see the results when they're done. You set these options in the Preferences window, which you reach either by choosing **VirusBarrier X6** > **Preferences...** or by pressing Command-comma.

General Preferences

The Preferences window is divided into six panes: **General**, **Modem**, **Log**, **Traffic**, **Whois**, and **Advanced**.

The top section of the General Preferences pane controls how the program looks to you; the bottom, how it sounds. Here's an explanation of each option.

The **Icon size** slider lets you choose how big you want icons to appear when you click **Select** on the **Overview** screen in order to scan files and folders for malware, and use Icon view, as well as for icon displays in the Quarantine Zone. (Changes to this setting have no effect when viewing items in List or Column view.)

The second option, **Show invisible items**, displays files that Mac OS X usually keeps hidden. These are typically files that are needed for your Mac to function properly, and that shouldn't be changed. Viruses and malware can hide in invisible files, so scanning them is of great importance. However, you don't need to show them to scan them: when you scan a folder, VirusBarrier X6 scans every item inside it, including invisible items.

Note that the Quarantine Zone always displays invisible items regardless of the setting in these preferences.

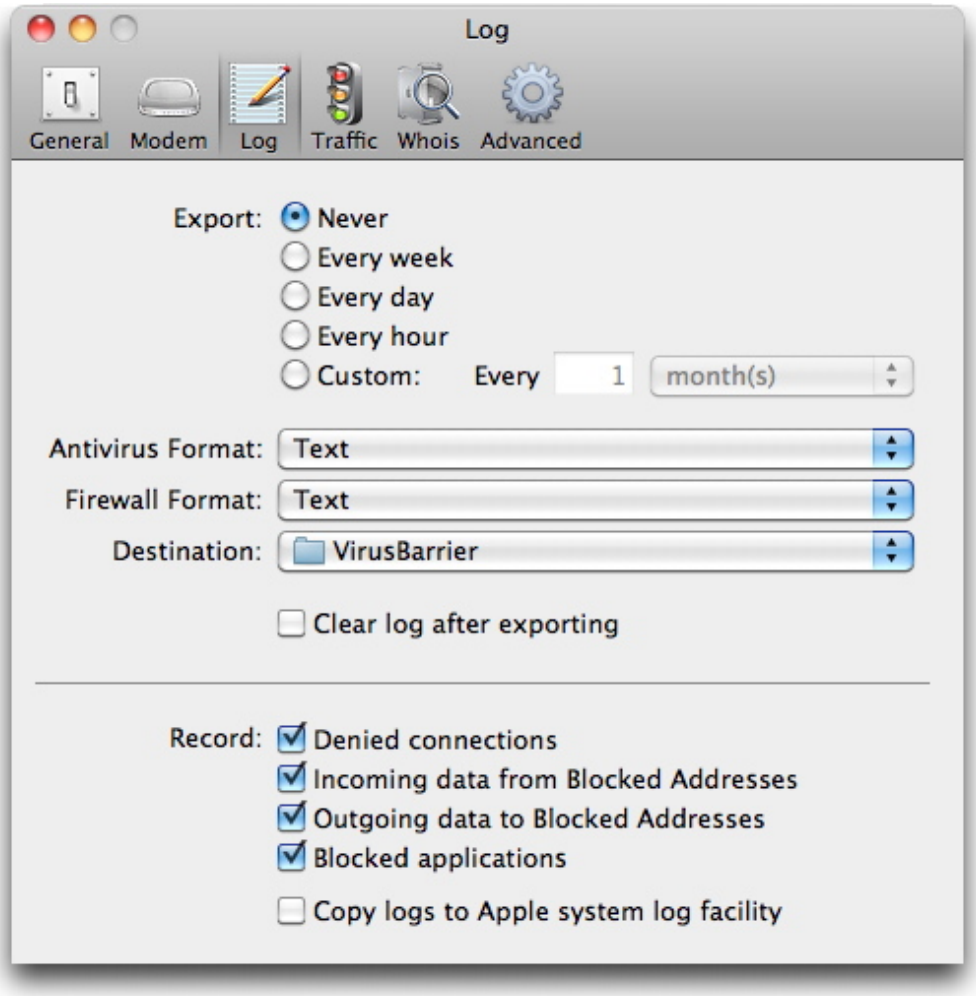
The **Sounds** section lets you control what you hear when VirusBarrier X6 detects or eradicates malware, when it finds a corrupted file, or when VirusBarrier X6 completes a scan without finding any malware. By default, these are set to speak their announcements: you can hear how they sound by clicking the appropriate popup menu and re-selecting **VirusBarrier Voice**. You can also change each sound by selecting any of the other sounds in that popup menu. To turn off any of the sounds entirely, select **None** from its popup menu.

Modem Preferences

You can use this option to provide total security for your modem, if you have one. To do this, click the **Modem** button on the Preferences screen. Securing your modem may prevent it from answering any calls. By clicking the Secure now button, you're telling VirusBarrier X6 not to accept any incoming calls: however, you'll still be able to make outgoing calls. To return your modem to its normal, unsecured state, click the **Reset** button.

Log Preferences

You can set VirusBarrier X6 to export its log at regular intervals. To do this, click the Log button on the Preferences screen.



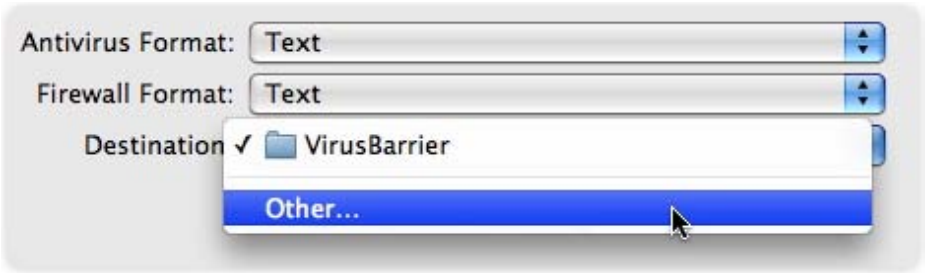
Your first choice is how often you'd like the log export to occur. If the **Every week** radio button is on, exports occur at midnight between Sunday and Monday; for **Every day**, they occur at midnight; for **Every hour**, they occur at the top of the hour. The **Custom** selection allows you to name a multiple of these times, for example once every two weeks. (The **Custom** selection also allows you to do the export once a month, at midnight on the first day.)

If your Mac is off or asleep when an export is scheduled, this procedure will occur when it is next turned on.

Antivirus logs can be exported in any of three formats; Firewall logs, in six formats. Click the **Format** popup menus to select the export format.

Note: for a description of Log export formats, see Exporting the Log later in this chapter.

You can select the folder where log export files are saved. By default, they are saved in the /Library/Logs/VirusBarrier folder. If you wish to have these files saved in another folder, select **Other...** from the popup menu and navigate until you get to the folder you wish to use. Then click **Select** to use this folder.



VirusBarrier X6 stores two Network logs. There is a rotating log, which contains a maximum of 4096 entries, which you see in VirusBarrier X6's Log panel. If automatic exports are enabled, a second log stores all entries. If you wish to retain full logs of all activity, you should therefore activate periodic exports. These logs are not limited by size (other than the available space on your hard disk). If you check **Clear log after exporting**, this will delete the log entries after each export so each new export contains only those entries recorded after the previous export. This setting only affects automated exports, and doesn't affect log exports done manually from the Log window.

You have a choice of which elements are recorded in your logs, as indicated by the checkboxes at the bottom of the Log preferences pane. The options are:

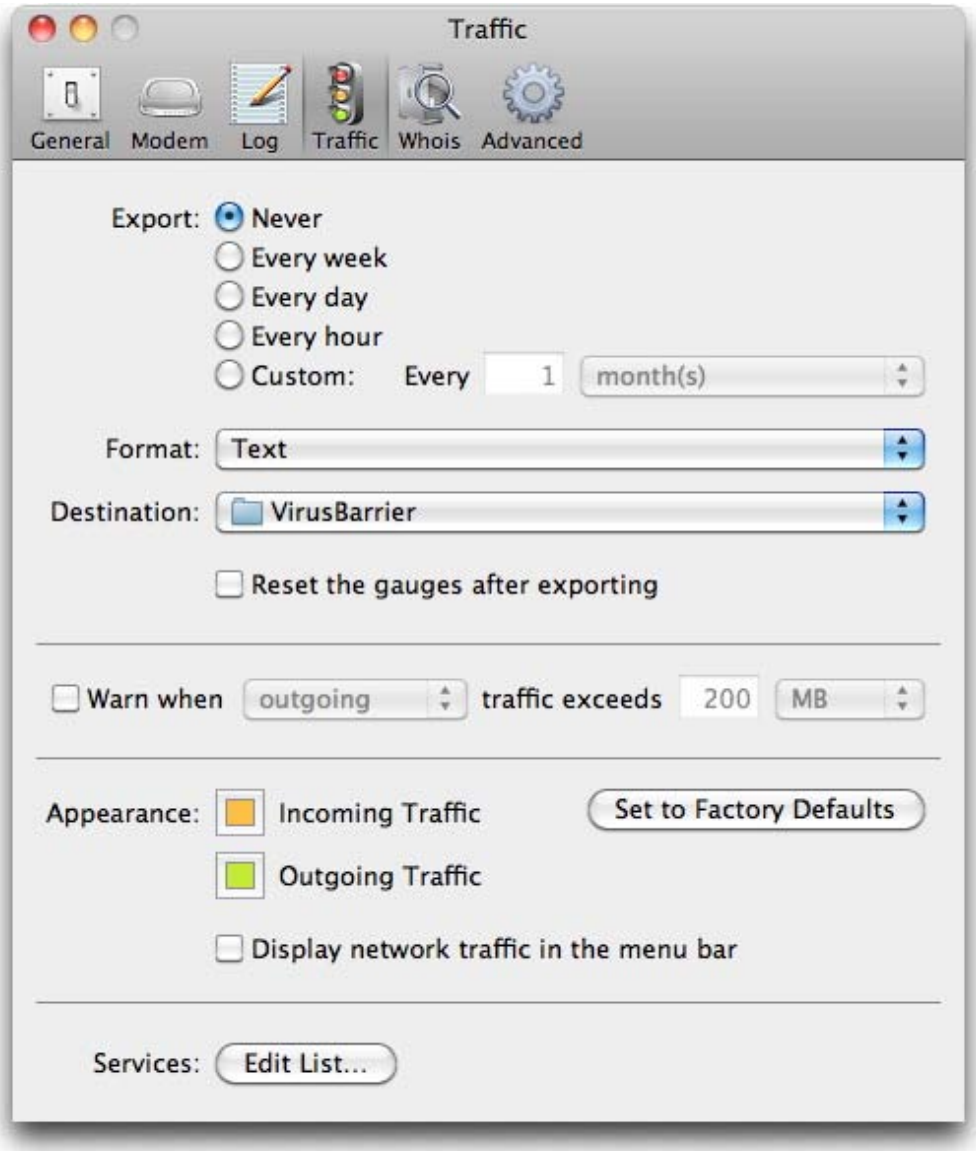
- **Denied connections**: Attempts to reach your Mac that were blocked because they violated rules you set up in VirusBarrier X6.
- **Incoming data from Blocked Addresses**: Attempts to send data to your Mac from hosts that are in the Blocked Addresses list.
- **Outgoing data to Blocked Addresses**: Attempts to send data from your Mac to hosts that are in the Blocked Addresses list.
- **Blocked applications**: Instances where VirusBarrier X6's Anti-Spyware prevented an application from communicating with the network.

The last checkbox is **Copy logs to Apple system log facility**. When checked, the Log data will be registered in the unified log system found in Mac OS X 10.5 and later; you can view these logs in the Console application, found in the

/Applications/Utilities folder.

Traffic Preferences

Like the Log preferences, the Traffic preferences screen gives you options to export traffic data at regular intervals. This screen also gives you several options for managing traffic data. To change these settings, click the **Traffic** button on the Preferences screen.



In the top section of this screen you control automated, periodic exports of traffic data. It works exactly the same as the log preferences: see the **Log Preferences** section above for details. The one setting that's different is the checkbox **Reset the gauges after exporting**, which in essence is the same as the log's **Clear log after exporting** checkbox. Checking it is the equivalent of clicking the **Reset** button next to the gauges to change total traffic to zero after automated exports. For more information about Traffic gauges, see Using VirusBarrier X6 Monitoring Tools.

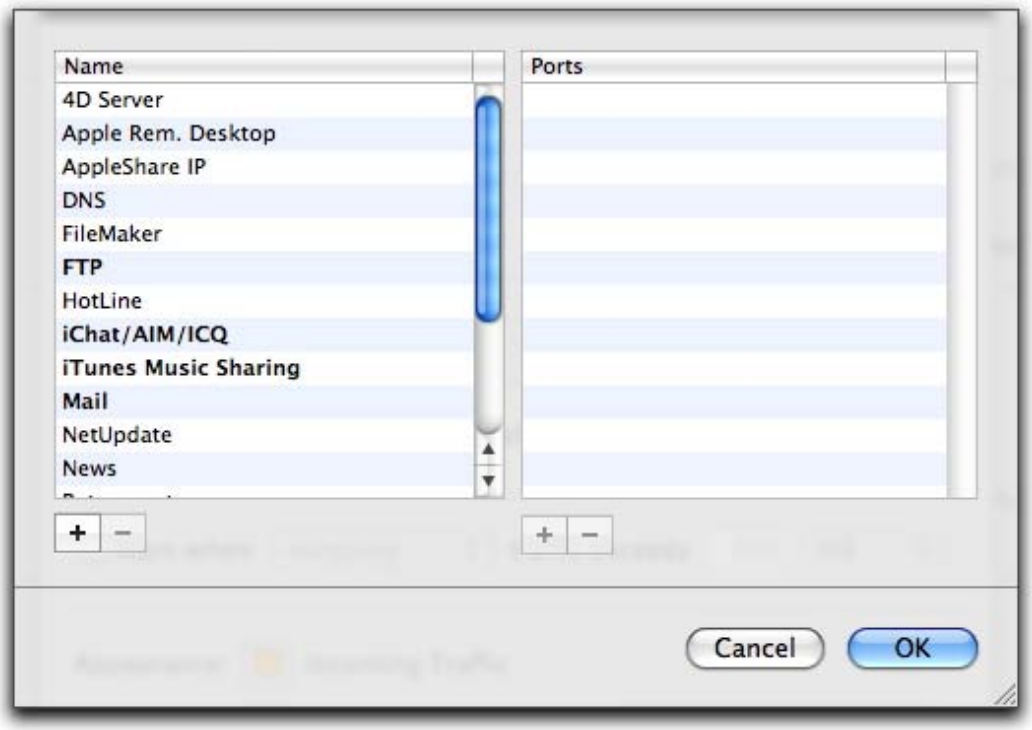
VirusBarrier X6's Traffic preferences include a setting that notifies you if the amount of data entering or leaving your computer goes above a certain limit. This can be very useful if you have an Internet access account with uploading or downloading restrictions.

If you check this option, VirusBarrier X6 displays a warning when your traffic exceeds the amount you have selected. You can choose to have a warning for **Incoming**, **Outgoing** or **Global** (total) traffic, and you can choose the threshold in kilobytes, megabytes or gigabytes.

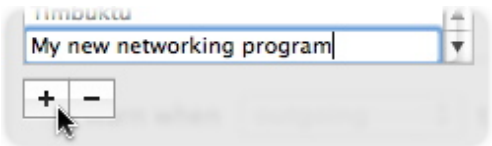
Below that is an **Appearance** section where you can change the color of incoming and outgoing traffic in all Traffic gauges and timelines. Clicking either colored box brings up a standard Mac OS X color picker: select your preferred color, then close the window by clicking the red Close button in the upper-left corner. The **Set to Factory Defaults** button returns the colors to orange for incoming traffic and green for outgoing traffic.

VirusBarrier X6 can display network traffic in the menu bar. Check **Display network traffic in the menu bar** to turn this feature on. This displays the amount of incoming and outgoing traffic at all times. You can turn this off by unchecking **Display network traffic in the menu bar**.

Finally, the Services button at the bottom lets you add, remove and change the kinds of traffic displayed in the Traffic gauges, which is very helpful if you're testing a new networking program. Clicking the **Edit List...** button opens a window that lists existing services



To add a service, click the + button in the lower-left corner, then enter the name of the service.

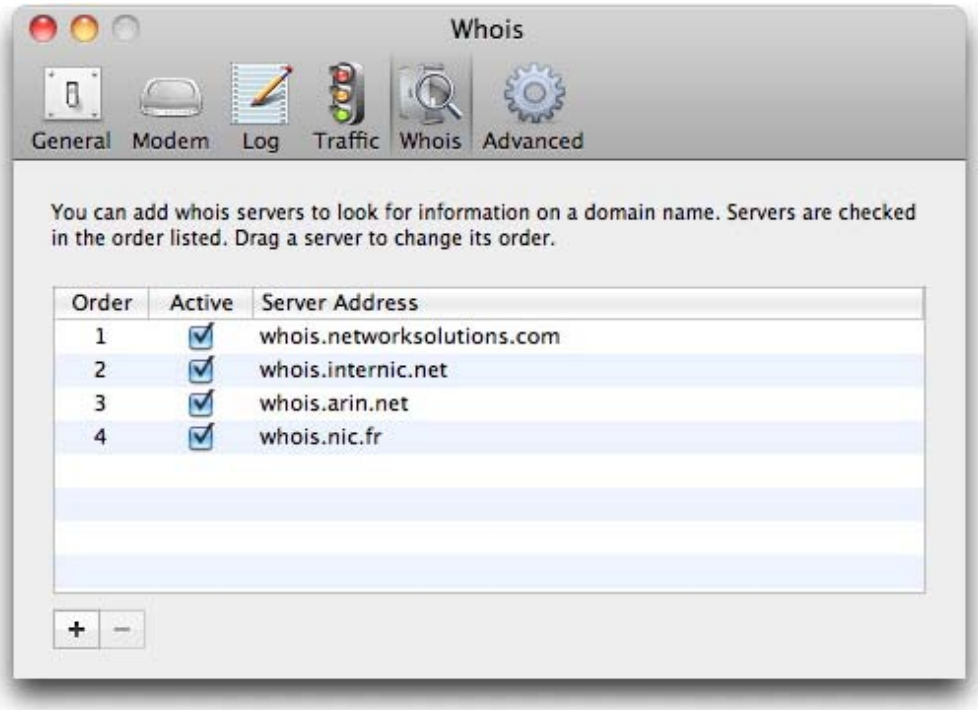


With that service highlighted, you then click the other + button, below the right column, to add ports that are associated with that program.

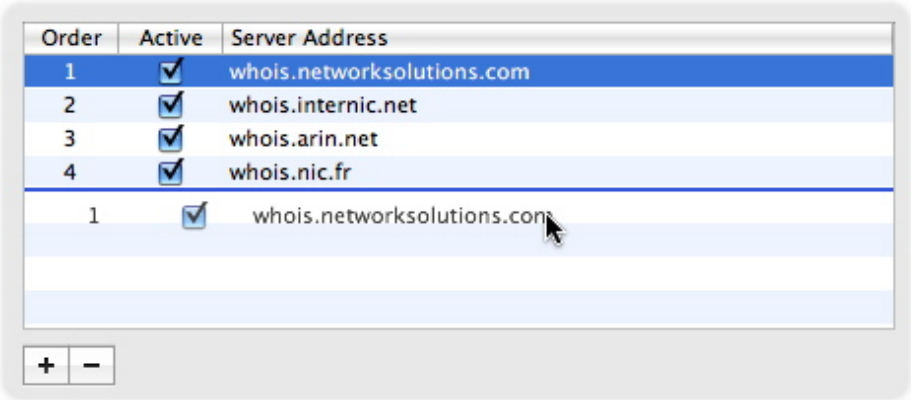
Similarly, you can edit or delete any services in the list that aren't listed in bold. Bold services such as Chat, Mail and Web are core to networking, and are therefore locked in place as a safety measure.

Whois Preferences

VirusBarrier X6's Whois function allows you to search for information on domain names and IP addresses. Four Whois servers are preset in this pane, and they are queried in the order shown in this panel.



If you wish to change their order, you can do so by selecting one of the servers and dragging it to a new location.



Adding new Whois servers to VirusBarrier X6 is easy: just click the + button and type in the name of the Whois server you wish to add.

You can also activate or deactivate the Whois servers in this panel. To deactivate a server, uncheck its checkbox. To activate a deactivated server, check its checkbox.

To remove a Whois server, select it by clicking it, and click the - button. A dialog box asks you for confirmation.

Advanced Preferences

Four options are available in the **Advanced** panel of VirusBarrier X6 Preferences.

- **Protection**: This is a simple **OFF**/**ON** slider, to quickly disable (or re-enable) *all* protections VirusBarrier X6 offers. Moving this slider to **OFF** completely turns off VirusBarrier X6, including the program's firewall logging. You will need an administrator's password to do this, or to change the slider back to **ON**. Regardless of the setting, VirusBarrier X6 will automatically be re-enabled when you restart your Mac.
- **Configuration**: Clicking the **Revert to Default...** button allows you to reset VirusBarrier X6 to its default configuration: "Client, local server" mode for the Firewall, with Antivandal and Privacy functions disabled. Regarding malware protection, these settings activate the Real-Time scanner, deactivate the scan of archives, and activate certain Advanced scanner settings. You will need an administrator's password to make this change. Doing so also clears all Firewall Modes and other settings you created, along with your Blocked Addresses and Trusted Addresses. It is recommended to export your current VirusBarrier X6 settings (**File** > **Export settings...**) before reverting to Default settings in case you want to recover your settings at a later date.
- **Setup Assistant**: Clicking the **Show Assistant...** button will launch VirusBarrier X6's Setup Assistant. See Getting Started with Intego VirusBarrier X6 for more information.
- **Security**: If you check **Always require a password to change settings**, only those users who can enter an administrator's password to make any changes to VirusBarrier X6's settings.

Working with Configurations

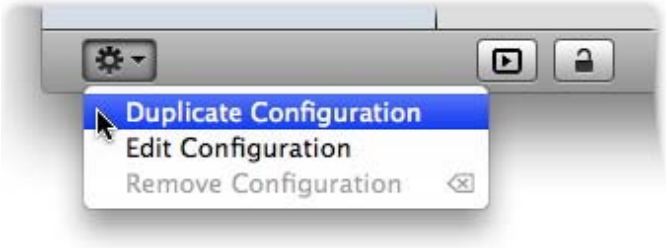
VirusBarrier X6 lets you save multiple configurations. Each configuration contains all the settings and preferences you have applied to VirusBarrier X6 in its different screens and preferences. You can make configurations for different locations, for example, one configuration when you're using your laptop at the office, and another for home use. You may want to have one configuration that includes additional protection for the times your Mac works as a server, and another for when it is a client. You may also want a specific set for less protection when you are connected to a local network, and additional protection when you are using public hotspots. You may want to have a configuration that sends you e-mail messages when any intrusions occur, for when you are not at your computer.

Configurations appear in a list on the left of every screen. A small action button below the list lets you duplicate, edit, remove and hide configurations. If you don't see the Configuration list, it might be hidden: display it by pressing Command-K, choosing **View** > **Show Configurations**, or clicking the Toggle Configurations button at the very

bottom-left corner of the window.

Creating, Editing and Deleting Configurations

The first time you use VirusBarrier X6 you'll see one configuration in the list, bearing the name you chose when you ran the Setup Assistant, or, if you did not run the Assistant, named "default." To create a new configuration, you duplicate an existing configuration by first highlighting it, then clicking and holding the action button (which looks like a gear), then choosing **Duplicate Configuration**.

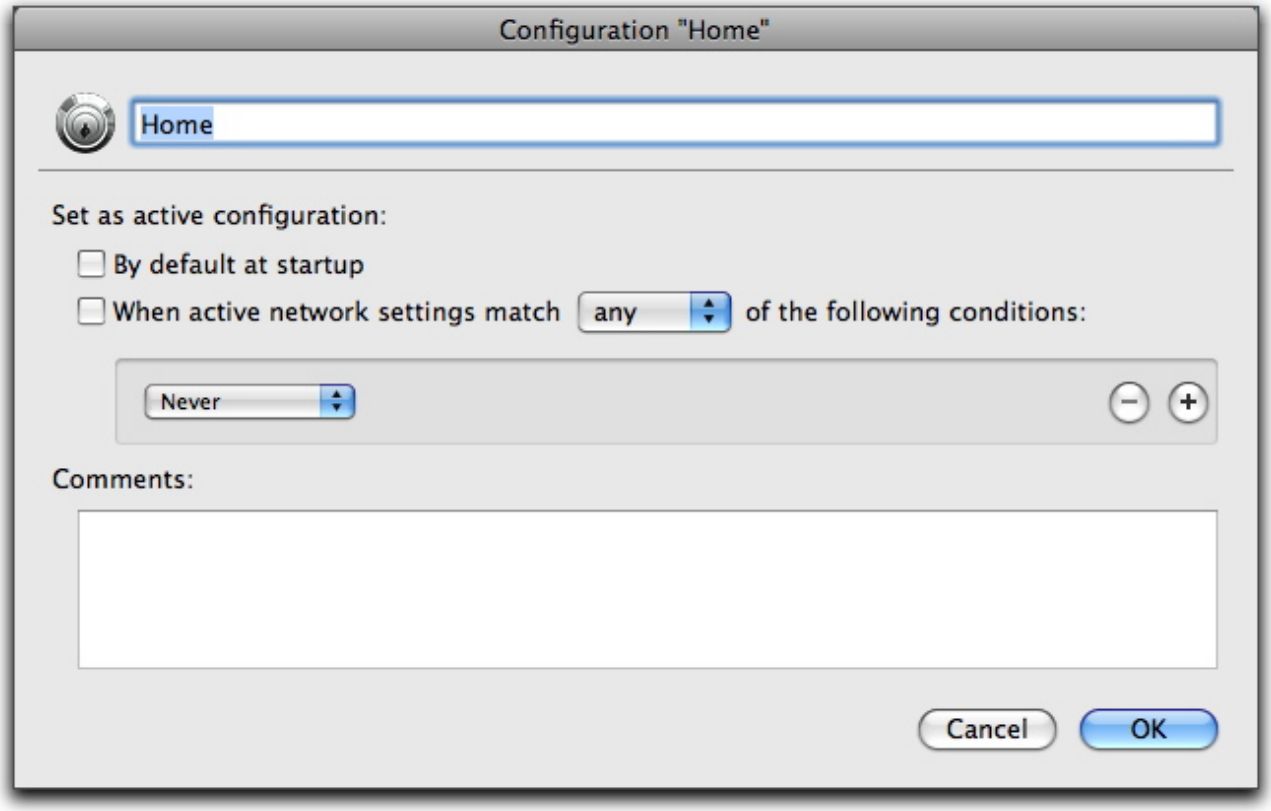


This new configuration has the same name as the one you duplicated, with the word "copy" appended. Rename the new configuration by double-clicking on it and typing a new name.

Now that you have a new configuration, activate it by clicking its radio button. Here, we've created two new configurations by duplicating "default" twice, renamed them, and selected the one named Home.

You can now make any changes to VirusBarrier X6 that you want, and they are saved under the current configuration. To make another configuration active, simply click its radio button. You can also select another configuration from the Configurations list in the Intego Menu. (For more information about the Intego Menu, see 2. Getting Started with Intego VirusBarrier X6.)

Once you've created a configuration, edit it by clicking the action button below the Configurations list and choosing **Edit Configuration**. You'll see a window like this:



This Configuration will become active when you turn on or restart your Mac if you check **By default at startup**.

In addition, by checking the **When active network settings match...** checkbox it will automatically become active when any or all conditions you specify regarding the following networking criteria are true.

- **Never**: This condition will never be true, so this prevents the configuration from turning on automatically.
- **Type**: Choices are **Ethernet**, **AirPort**, **FireWire**, **PPP** or **Bluetooth**.
- **IP Address**: You can choose a specific IP address, or a range. A **Current** button identifies the IP address your Mac has at the moment.
- **AirPort SSID**: The common name for a wireless network, such as "My AirPort." You can choose for this condition to be true when the SSID is, is not, or contains a text string you specify.
- **AirPort BSSID**: The MAC address of a wireless network connection point, expressed as a string of hexadecimal numbers.
- **Location**: The Location defined in your Mac's Network preferences.
- **Always**: The condition is always true.

The Comments field is a place for any description or notes you'd care to add: they don't affect operation of the configuration in any way.

There are two ways to delete a configuration. First, click it once to highlight it; then, either click the action button below the configuration list and choose **Remove Configuration**; or, press Command-Delete. In either case, a dialog box asks you to confirm the deletion. You can't remove the active configuration: instead, you must switch to another before removing it.

Exporting and Importing Settings

You can save all your VirusBarrier X6 settings in a special file that you can then use to import these settings into another copy of VirusBarrier X6. This is especially useful if you manage many computers and want to use the same settings for all of them.

To export your settings, select **File** > **Export Settings...**. A dialog box asks you to name the settings file and choose a location to save it. Click Export when you have finished. The result is an XML file that can be imported into any copy of VirusBarrier X6, including the one that created it.

To import settings, select **File** > **Import Settings...** A file dialog asks you to locate the settings file. Once you have located the file, click Import and these settings are immediately applied to VirusBarrier X6. You can also double-click a VirusBarrier X6 settings file to import it.

‹‹ Using VirusBarrier X6 Monitoring Tools

Appendix: Creating Custom Firewall Rules ››

© 2011 Intego. All Rights Reserved.

Creating Custom Firewall Rules

- Custom Firewall Rules
- Creating Rules with the Assistant
- Creating Service-Specific Rules Quickly
- Creating Rules Manually
- Working with Rules

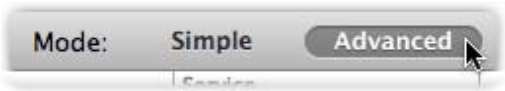
Go to Main Table of Contents

Custom Firewall Rules

Each of the five firewall settings described in chapter 4, Protecting Your Mac from Network Attacks, is actually a collection of rules, each of which in turn is defined by naming permitted or forbidden sources, destinations, services and interfaces.

Simple mode doesn't permit you to change the rules or any of their parts. To do that, you need to enter the Firewall screen's advanced mode. To do so, click the **Firewall** button at the top of the main screen.

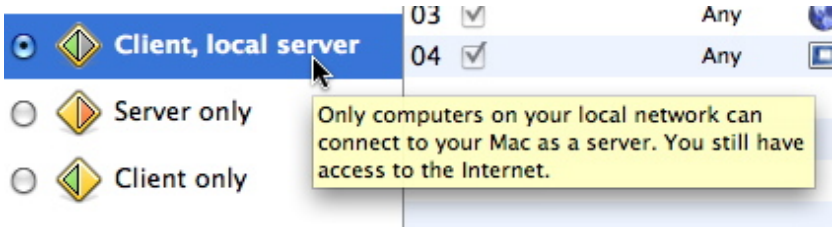
Then, click the **Firewall Rules** tab, if it's not active, and the Advanced Mode button in the upper-right corner.



WARNING: Changing these settings could dramatically affect your computer's ability to access local networks and the Internet. You should only use advanced mode if you fully understand its effects and how it functions.

In simple mode, clicking any of the five preset firewall settings displays an animation; in advanced mode, you see the details of each setting's rules.

In addition, hovering the cursor over any of the preset settings for a few seconds displays a text that briefly describes what it does.


Client, local server
Server only
Client only
03 Any
04 Any
Only computers on your local network can connect to your Mac as a server. You still have access to the Internet.

In this example, the "Client, local server" setting shown has four rules. The first allows the local network to access your Mac through all Connected Services - that is, TCP connections that involve back-and-forth communications, such as serving files from your Mac. The second rule, however, forbids such connections from the Internet at large, preventing your Mac from acting as a server to an unknown computer outside your local network. The third rule allows all other communications from the Internet to your Mac, while the fourth allows all communications from your Mac *to* the Internet.

The five preset firewall settings are "frozen" for convenience and stability: you can't change their rules, or the order in which they appear. But VirusBarrier X6 gives you two ways to create additional, customized settings: through the program's Firewall Assistant, and manually.

In either case, the first step is to click the + button below the list of settings. You'll see a new setting appear, named "untitled settings". Click it and type any name you prefer, then press Enter or Return to make the change permanent.

Note that you have only created this setting, but have **not** enabled it yet. It's a good idea to not enable firewall settings until you have finished adding all your rules. To make it the active setting, click the radio button to its left.

Creating Rules with the Assistant

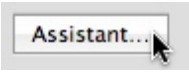
VirusBarrier X6 contains an assistant to help you create your own custom firewall rules. With this assistant, you can create your own rules with just a few mouse clicks. While not all of VirusBarrier X6's rule features are available when you create rules with the assistant, it can cover most of your needs for firewall rules. If you need more customization, you can create rules using the assistant then edit them manually.

The VirusBarrier X6 Assistant walks you through a series of steps to create your rule:

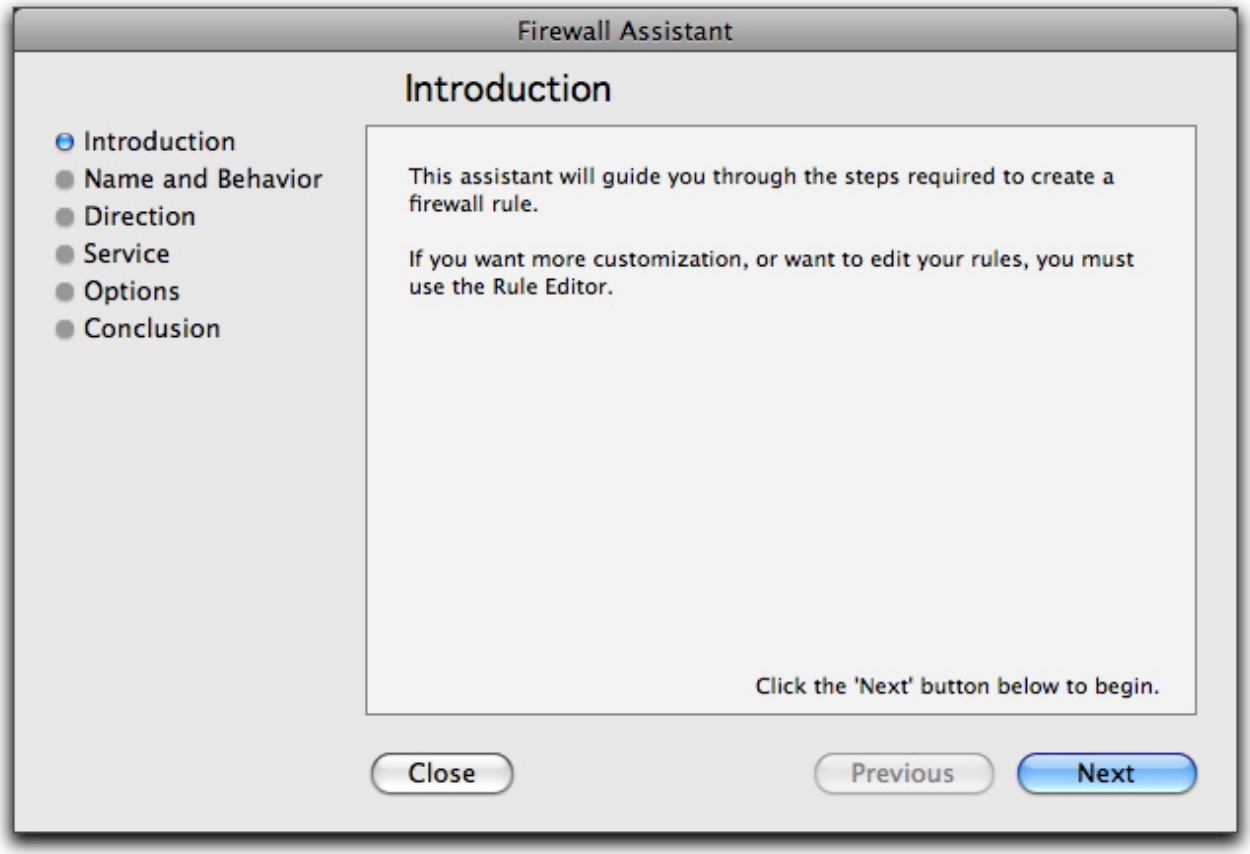
- **Introduction**
- **Name and Behavior**
- **Direction**

Service
- **Options**
- **Conclusion**

To create a new rule using the assistant, click the **Assistant** button.

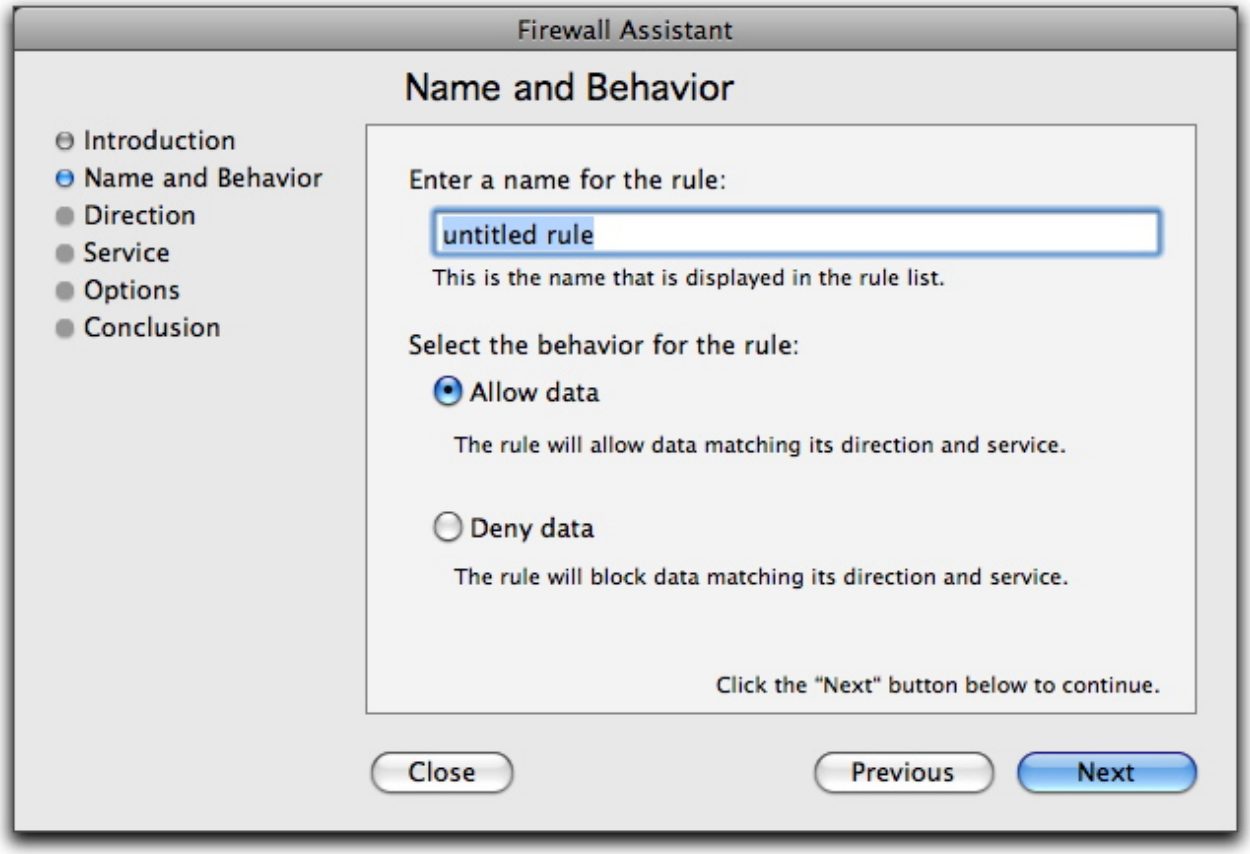


The first assistant screen displays.



Click the **Next** button to begin creating a new rule. You can click the **Previous** button at any time to return to previous screens, or click **Close** to exit the Assistant.

Name and Behavior

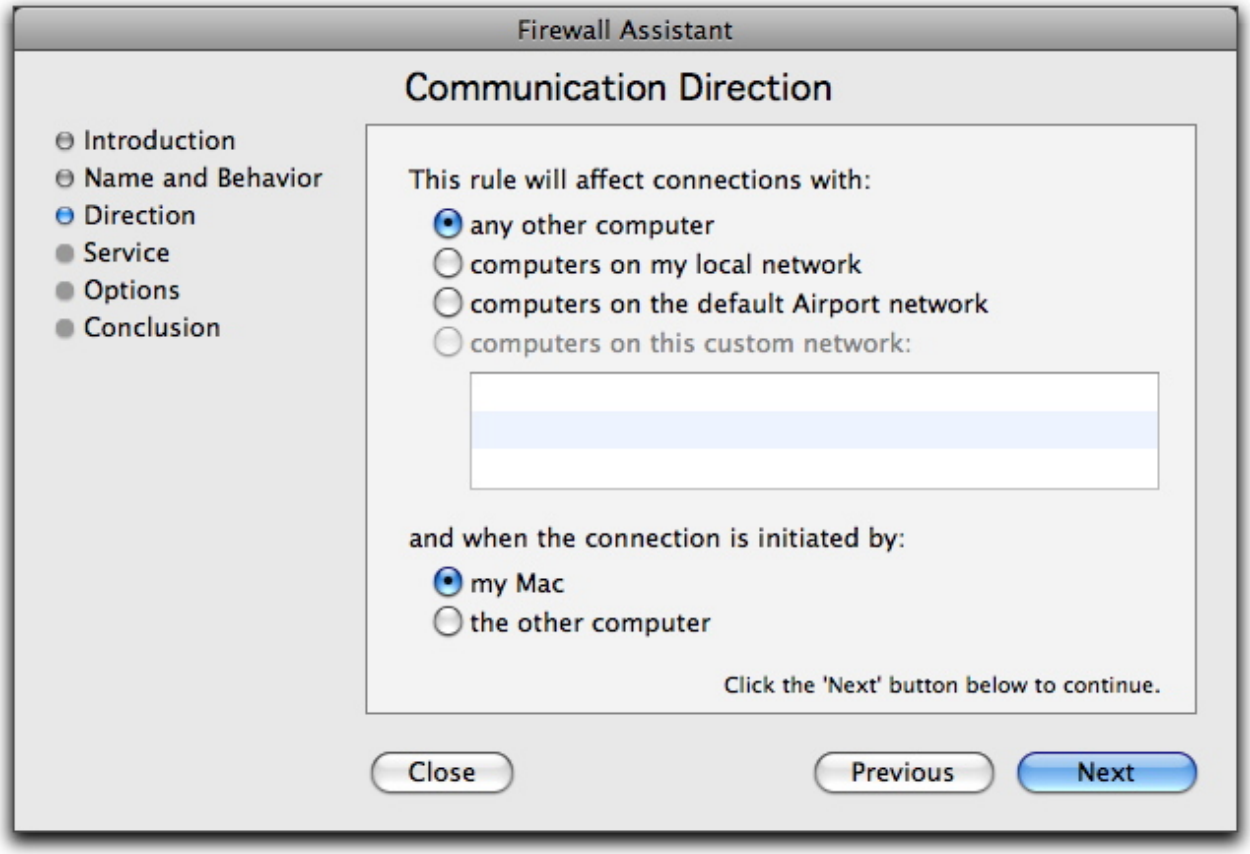


Enter a name for your rule in the name field, then select the behavior for the rule: **Allow data** or **Deny data**. If you select **Allow data**, the rule will allow data matching its direction and service to pass. If you select **Deny data**, the rule will block data matching its direction and service.

Click the **Next** button to go to the next screen.

Communication Direction

This screen lets you choose the communication direction and which host initiates the communication.



First, in the **This rule will affect connections with:** section, select a remote host. You have four choices for the remote host:

- **Any other computer**: Any computer other than your Mac.
- **Computers on my local network**: Any computer on the same local network as your Mac.
- **Computers on the default AirPort network**: Any computer on your default AirPort network, if you have one.
- **Computers on this custom network**: If you have created any custom networks using the standard rule editor, you can select one of them here.

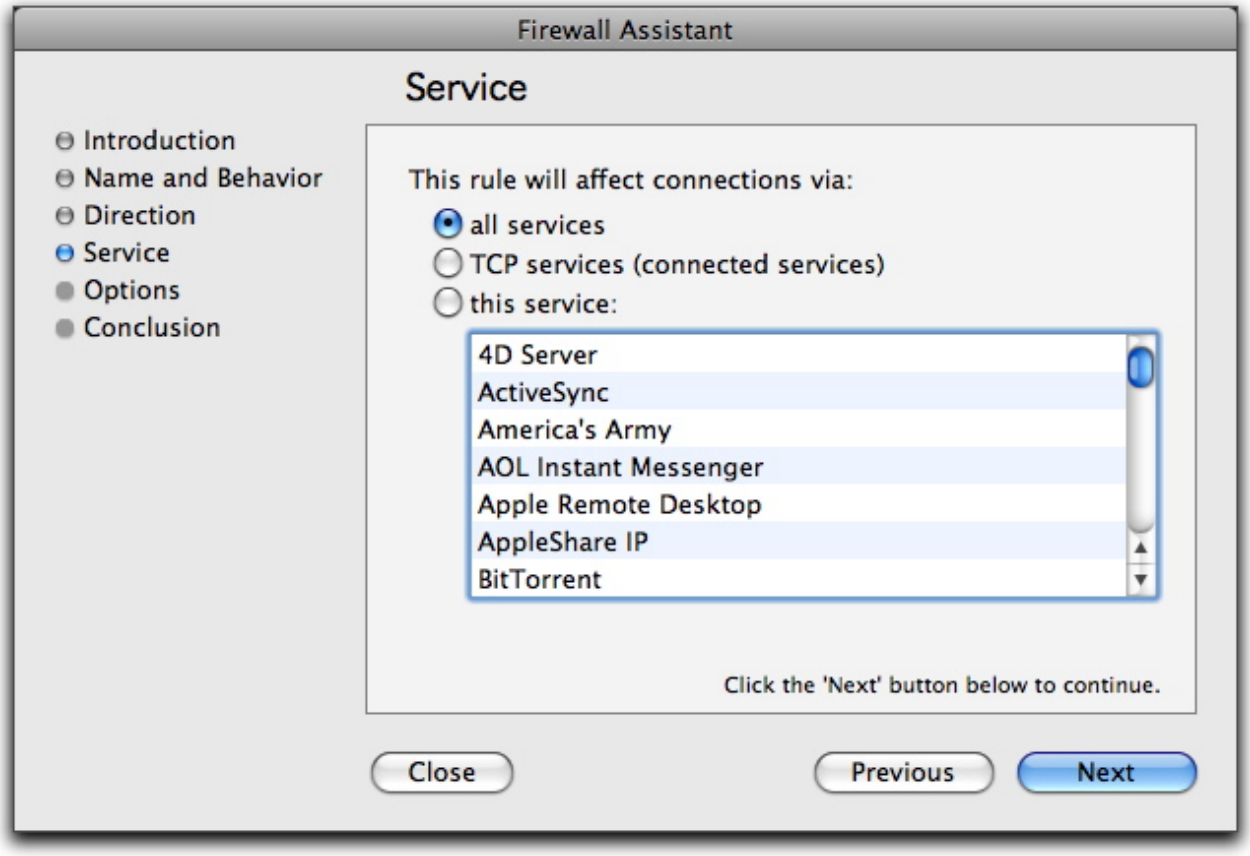
Next, select the computer that initiates the connection:

- **My Mac**: The computer using this rule.
- **The other computer**: The remote host, as was defined in the first part of this screen.

When you have finished, click the **Next** button to go to the next screen.

Service

This screen lets you choose the service that the rule affects.



You can choose from three types of services:

- **All services**: All network services.
- **TCP services (connected services)**: Services that require that a connection be open and maintained between two computers, such as HTTP, FTP, Telnet, SSH, POP3, AppleShare, etc. This covers all TCP connections.
- **This service**: You can choose from a list of services that correspond to popular applications and protocols. Select the service you want to use by clicking its name in the list.

When you have finished, click the **Next** button to go to the next screen.

Options

This screen lets you choose additional options for your rule.

Firewall Assistant
Options
Introduction
Name and Behavior
Direction
Service
Options
Conclusion
Select additional options for this rule:
Log rule usage
When data packets match the rule, the Firewall records this in its log to show that the rule was used to filter the packet.
Disable the rule
The rule will be created but the Firewall will not use it until you enable it.
Click the 'Next' button below to continue.
Close
Previous
Next

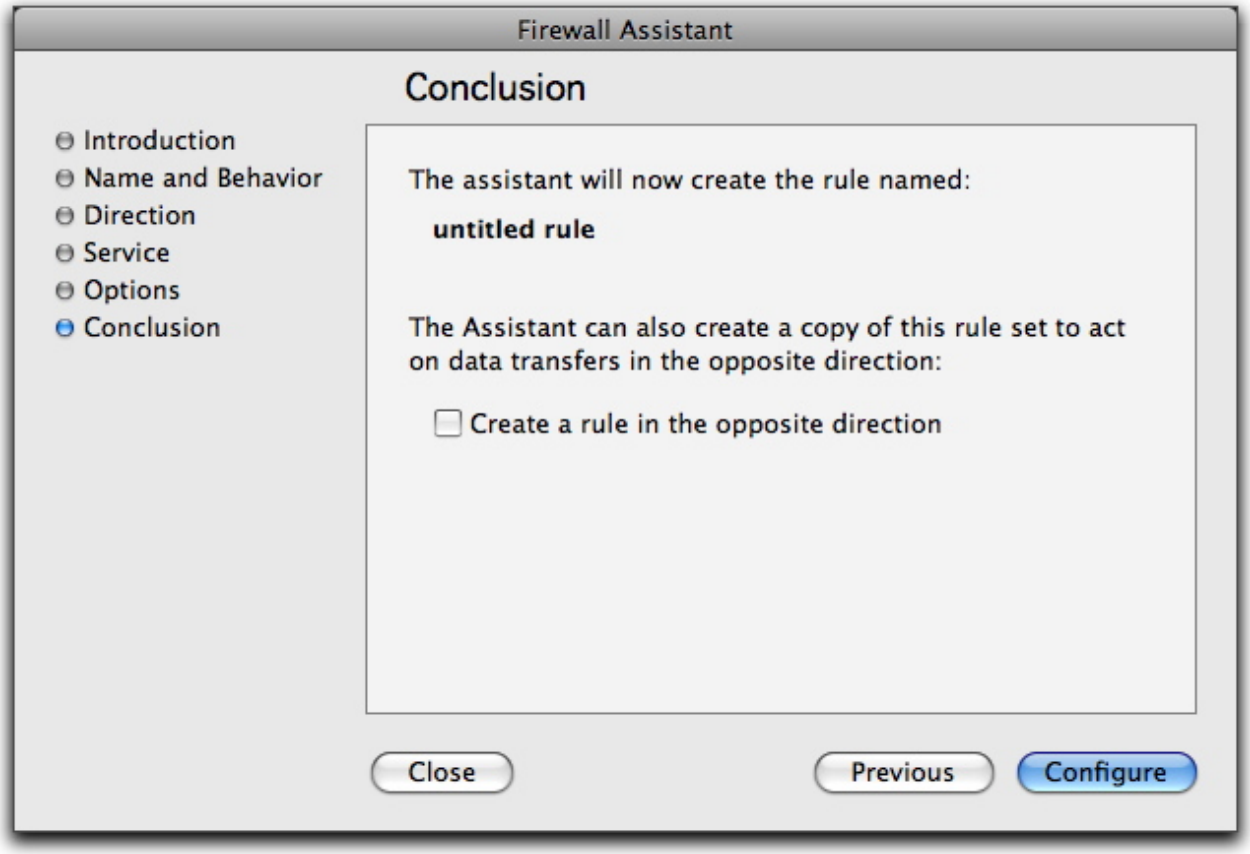
Two options are available on this screen:

- **Log rule usage**: The firewall records each time this rule is used in its log.
- **Disable the rule**: VirusBarrier X6 creates the rule but disables it. You can enable it manually.

When you have finished, click the **Next** button to go to the next screen.

Conclusion

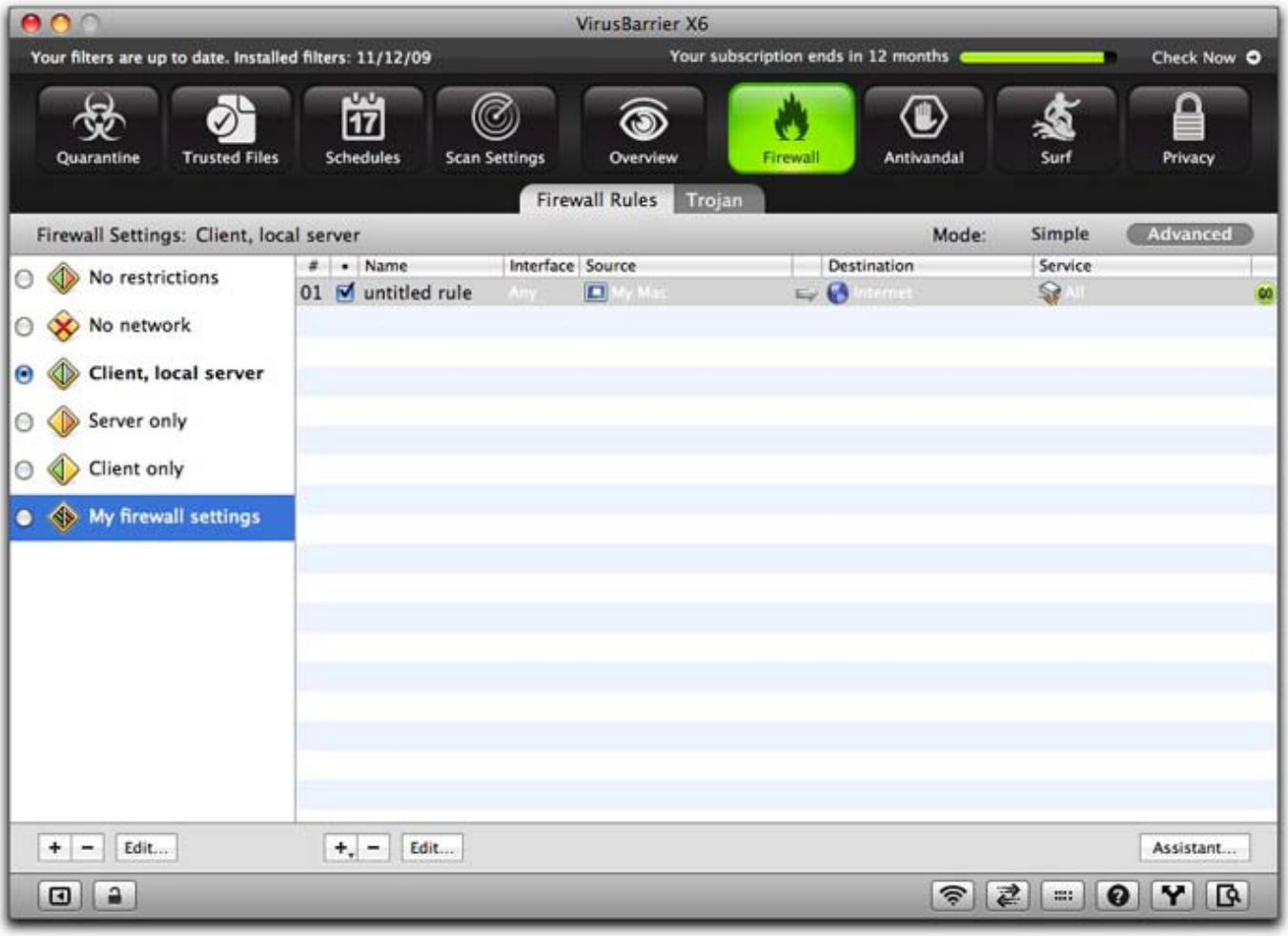
This screen creates the rule according to the settings you have selected in the assistant.



This screen offers one final option: if you check **Create a rule in the opposite direction**, the assistant creates a matching rule with the source and destination switched.

Click **Configure** to create your rule and exit the assistant.

When you have finished, you will see that your rule (or rules, if you checked **Create a rule in the opposite direction**) displays in the VirusBarrier X6 list of firewall rules.

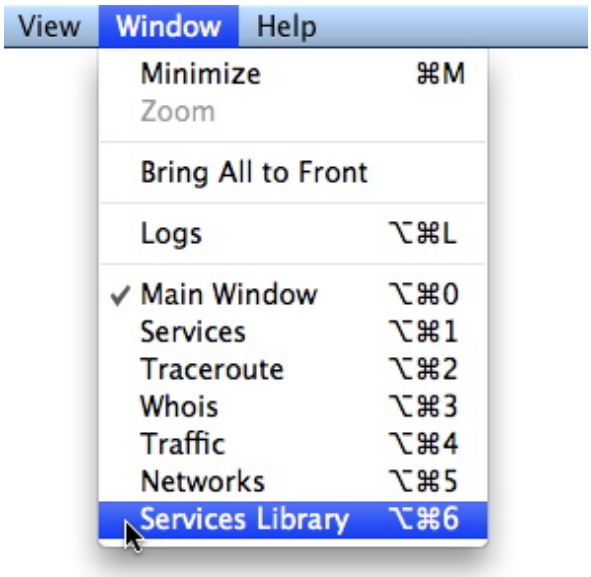


If you wish to further customize the rule, or edit it, see below, **Editing Rules**.

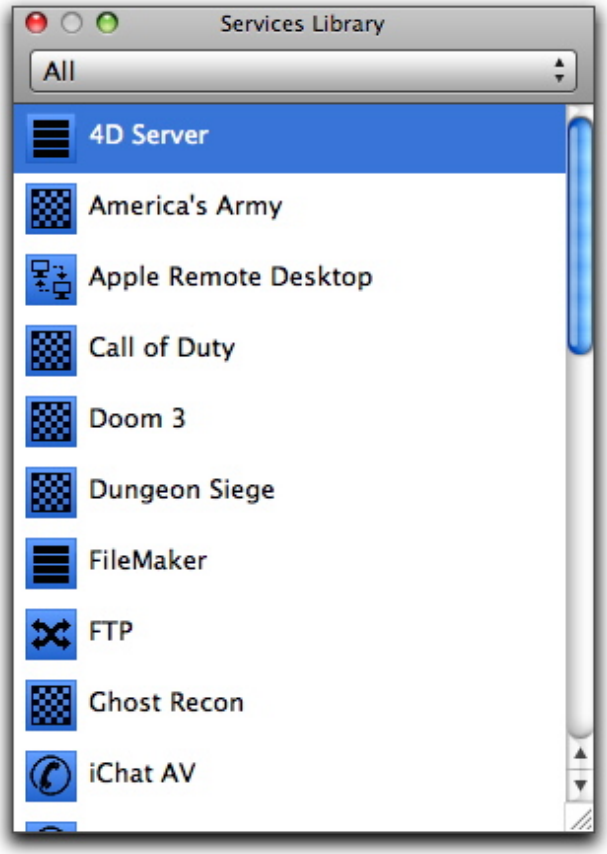
Creating Service-Specific Rules Quickly

There are two ways to quickly create rules to control information to and from common services and programs. The first is by clicking the + button at the bottom of the Rule list and holding your mouse button down for a second. You'll be able to choose from a popup list of the most common services. A rule governing your selection then appears in the Rules list.

The second way to quickly create service-specific Rules is with the Services Library. To display the Services Library, choose **Window** > **Services Library**, or press Option-Command-6.



The Services Library window opens and displays a list of the most common services.



To create a new rule, select the desired service and drag it to the rule list. By default, rules added in this way allow all traffic from your Mac to the Internet, on all interfaces. In other words, the rule doesn't prohibit any activity until you edit its settings, as is described below.

Creating Rules Manually

You can create individual rules using the Rule Editor. Click the + button at the bottom of the list of rules and the Rule Editor displays.

VirusBarrier X6's Rule Editor allows network administrators to quickly and easily define and implement a comprehensive security policy. It is extremely flexible, and allows you to define an unlimited number of rules in seconds. To create a rule, you need to specify details in six areas:

- **Rule Name, Logging, Evaluation and Schedule**
- **Rule Source**
- **Rule Destination**
- **Rule Service**
- **Rule Interface**
- **Rule Action**

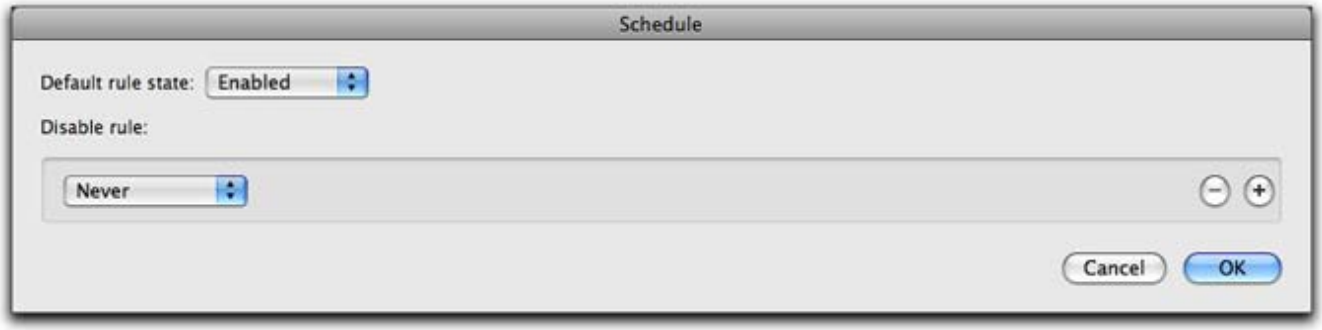
Rule Naming, Logging, Evaluation and Schedules

At the top of the Rule Editor is a field where you can name this rule. Just below it is the **Log** checkbox. If you check the **Log** box, an entry is added to the VirusBarrier X6 log any time this rule acts; a small red dot to the right of the rule's name in the Rules list indicates that the rule is logged. If this box is not checked, this rule is not logged.

If the **Log** checkbox is checked, the **Stop Evaluating Rules** checkbox will be available, and is checked by default. These two settings, in tandem, are a powerful way to troubleshoot a network without hampering its traffic.

WARNING: If you can't figure out why some of your rules aren't taking effect, look at the rules above it and ensure that the Stop Evaluating Rules checkbox is off for each of them.

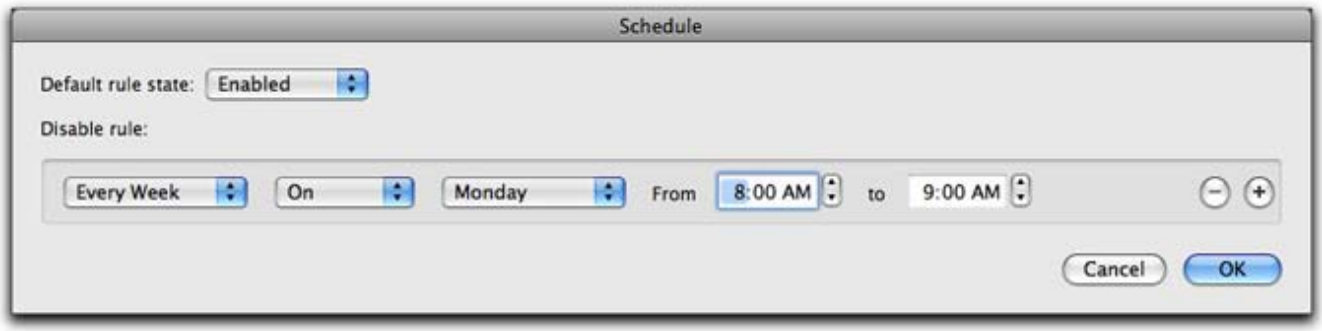
To edit the Schedule, click the **Edit...** button. The Schedule window displays.



The **Default rule state** is set to **Enabled**, which means that your rule is activated. If you set it to **Disabled**, VirusBarrier X6 does not use this rule. You may want to have certain rules active in one configuration, and not another. For more on using configurations, see chapter 6, Preferences and Configurations.

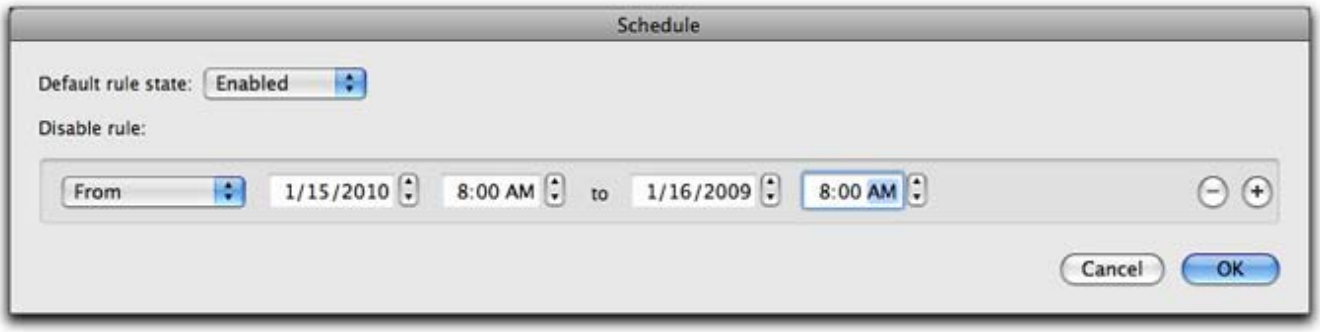
If your **Default rule state** is **Enabled**, you can set specific times for the rule to be disabled. If your **Default rule state** is **Disabled**, you can set specific times for the rule to be enabled.

When you first create a rule, the rule will always be active. If you wish to have the rule enabled or disabled at certain times, click the popup menu for either **Enable rule** or **Disable rule**, depending on which **Default rule state** you have chosen, and select one of the time intervals in the list.

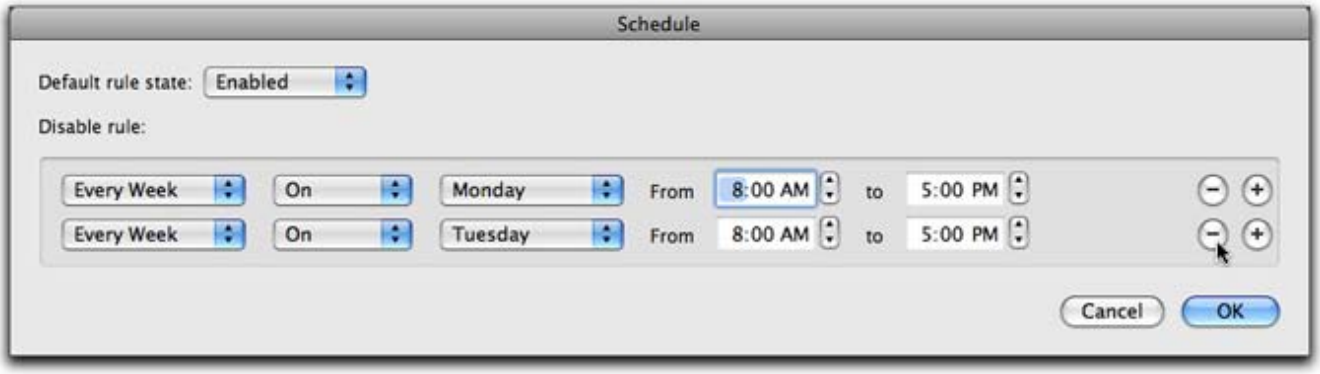


Three options are available in addition to **Never**.

- **Every Week** allows you to change the rule's schedule so it is enabled at a fixed time every week, such as every Monday at 8:00 am.
- **Every Day** enables the rule at a specific time every day.
- **From** allows you to disable or enable the rule for a specific period of time by specifying the beginning and ending time.



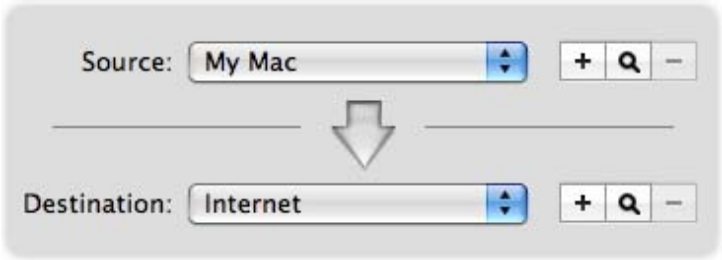
You can schedule additional times for rules to be enabled or disabled using the + button. For example, if you need a rule to be disabled only on Mondays and Tuesdays, you can set these two days in the Schedule window. To remove a scheduled time from the list, click the – button to the right of the item.


Schedule
Default rule state: Enabled
Disable rule:
Every Week On Monday From 8:00 AM to 5:00 PM
Every Week On Tuesday From 8:00 AM to 5:00 PM
Cancel OK

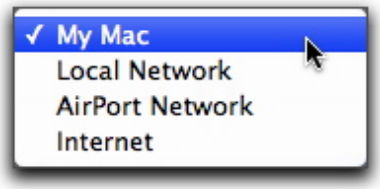
Scheduled rules are displayed with a calendar icon in the rule list. This particular rule also has logging turned on, as indicated by the small red dot next to its name.

Rule Sources and Destinations

When defining rules, the **Source** is the entity that sends data; the **Destination** is where the data goes. You can choose from a list of four sources and destinations for any rule. However, VirusBarrier X6 will not allow you to choose the same source and destination for a given rule. (If you try, VirusBarrier X6 will correct the error.)



These four Sources and Destinations are available by default:



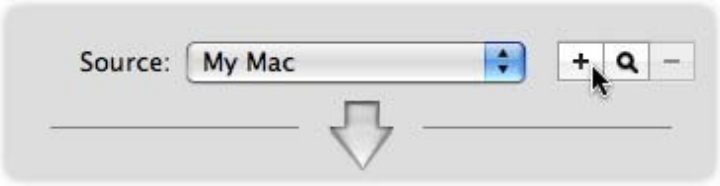
My Mac: Your computer.

- **Local Network**: A local network that your computer is connected to.
- **AirPort Network**: A wireless AirPort network that your computer is connected to.
- **Internet**: The Internet, in addition to any local network you may be connected to; effectively, all networks.

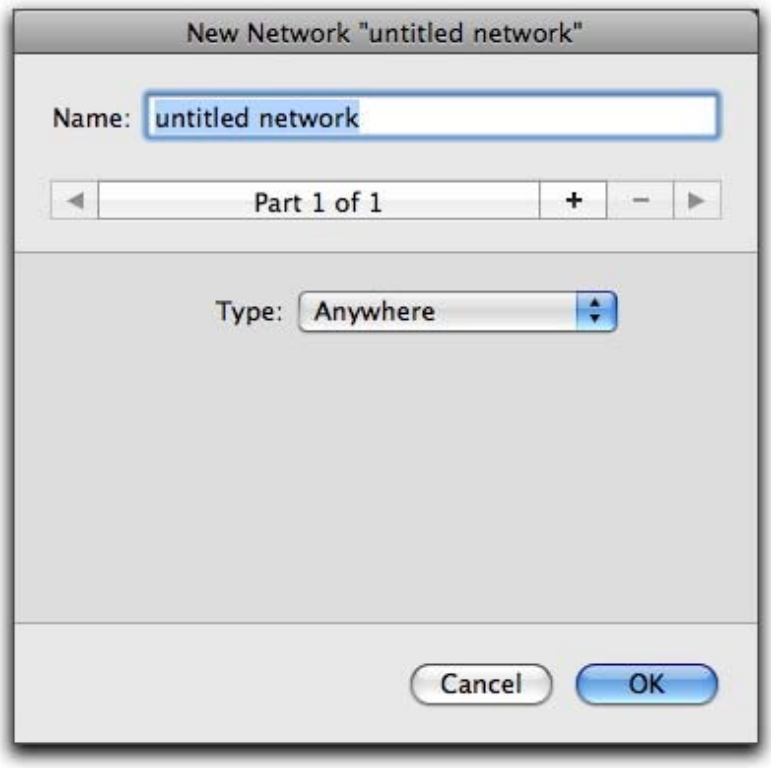
Creating New Sources and Destinations

You can create new sources and destinations to use in your rules. This allows you to specify exactly which computers you wish to have your Mac communicate with.

To create a new source, click the + button to the right of the **Source** or **Destination** popup menu. In our example, we'll create a new Source; however, once it's created, it will also show up in the list of possible Destinations.



The New Network editor displays.



Enter a name that will help you remember the network. If, for example, you're blocking IP addresses whose last octet is in the range of 100-155, you might name the Source/Destination "IPs from 100-155".

The pop-up menu offers a selection from seven types of network.

Name	Definition	Address Type
Anywhere	Any network.	None, as this source covers all networks.
My Mac	Your computer.	The IP address(es) of your Mac displays in the Address field, and cannot be changed.
My local network	The local network your computer is connected to.	The IP address(es) of your Mac and subnet mask of your local network display in the Address field, and cannot be changed.
Machine	A specific IP address.	Any IP address. If you enter a domain name, VirusBarrier X6 will resolve it to a single IP address.
Network	A specific network.	Any Subnet IP address and Subnet mask. As above, VirusBarrier X6 will resolve domain names to a single IP address.
Address Range	A group of IP addresses.	Beginning and ending addresses. VirusBarrier X6 will resolve domain names to a single IP address.
Ethernet ID	A single device connected to the network by Ethernet.	An Ethernet ID, as six two-character hexadecimal numbers.

Rule Services

A "Service" is a combination of protocol type, port (or ports) used, and protocol-specific criteria. These items, taken together, typically describe a program or class of program that sends and receives information. For example, information sent by the TCP protocol over port 80 using HTTP would be a Web service.

VirusBarrier X6 comes with over 50 common services preprogrammed so you can easily stop (or allow) traffic that appears to be of a specific type.

While most preprogrammed Services clearly map to a specific program, some selections in this list such as "Web" pertain to a class of communications instead. Here are some of those non-specific Services:

Name	Description	Settings
All	All communications, regardless of protocol or port.	All protocols, on all ports.
Apple Remote Desktop	A program that allows an administrator Mac to control another Mac over a network connection.	Port 3283 over UDP.
Connected Services	All TCP communications. A TCP session maintains a connection between computers, so it's always clear that it was initiated by the Mac and can therefore be trusted. By comparison, a UDP session is a series of communications without a "memory" of who initiated it.	All TCP communications, on any port.
FTP	File Transfer Protocol.	TCP, ports 20 or 21.
iChat AV	An instant messaging program with video and sound.	Port 5060 over UDP.
IRC	Internet Relay Chat.	TCP on port 194 for IRC, and all TCP traffic between ports 6665

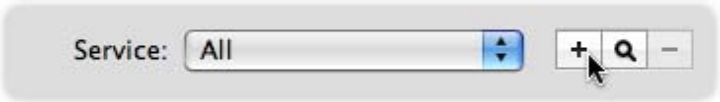
		and 6669, inclusive.
iTunes Music Sharing	A way to share your iTunes music library over your local network.	Port 3689 over TCP.
Mail	E-mail communications.	TCP port 25 for SMTP, port 110 for POP3, port 143 for IMAP4, port 220 for IMAP3 port 389 for LDAP, and port 587 for message submission.
NTP	Network Time Protocol.	UDP on port 123.
SSH	Secure Shell.	TCP on port 22 using SSH.
Telnet	Remote login.	TCP on port 23 using telnet.
VNC	Virtual Network Computing, a graphical remote-control system.	TCP on ports 5900-5999.
Web	Web browsing, for example through a browser such as Safari.	TCP on ports 80 and 8080 through HTTP, and on port 443 on HTTPS.
Well-Known Ports	A large range of ports with long usage traditions in network communications.	TCP and UDP on all ports from 0 to 1023.

The remaining services are for specific programs or protocols.

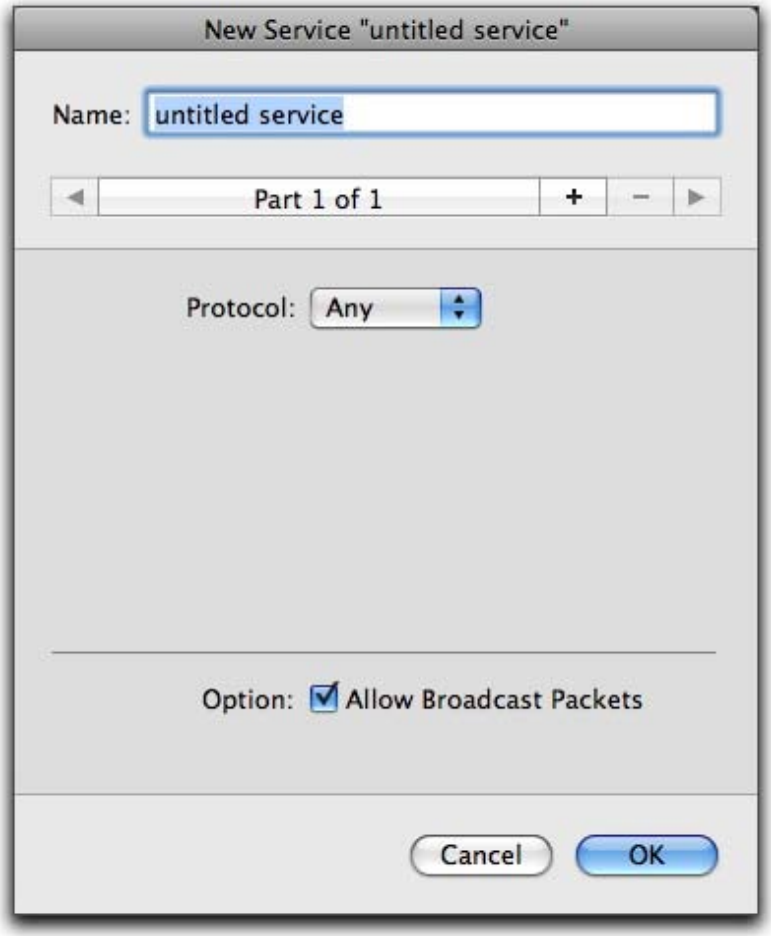
Be careful when creating rules for specific services. When you select a service for a specific program, it is possible that this program uses the same port as another program or service. Blocking or authorizing a specific service may conflict with other, more general rules. For example, if you wish to block ICQ traffic, selecting **ICQ** as a service will also block AOL Instant Messenger traffic since both programs use the same port. Other programs may also share the same ports. If you find that you cannot connect to a given service, or send or receive traffic, try deactivating your rules one by one to see if there is a conflict.

Creating New Services

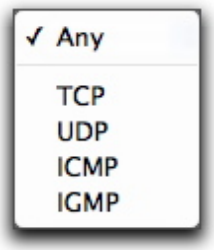
To create a new service, click the + button next in the **Service** section.



The New Service editor displays.



Four different protocol suites are available from the Protocol pop-up menu: **TCP**, **UDP**, **ICMP** and **IGMP**. You can also select **Any**, which covers all protocols.



When you select one of these protocol suites, additional options display in the bottom section of the panel, with a list of services that you can select from. The options depend on the protocol you selected.

TCP or UDP have the following options:

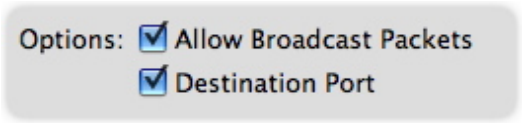
- **Any port**: Affects all ports.
- **Single Port**: Lets you specify a single port either by typing its number or by selecting from over a hundred options in the popup menu. (VirusBarrier X6 automatically fills in the correct number when you select from the popup menu.)
- **Range of Ports**: Lets you enter the beginning and ending port numbers that define a range.

ICMP or IGMP have the following options:

- **Any**: Affects all types.
- **Specific Type**: Lets you specify a single value either by typing its number or by selecting from over twenty options in the popup menu. (VirusBarrier X6 automatically fills in the correct number when you select from the

popup menu.) You can also specify a Code number, if necessary.

For each of these, an option is available to **Allow Broadcast Packets**. If checked, packets sent to all computers on a local network are included in this service.



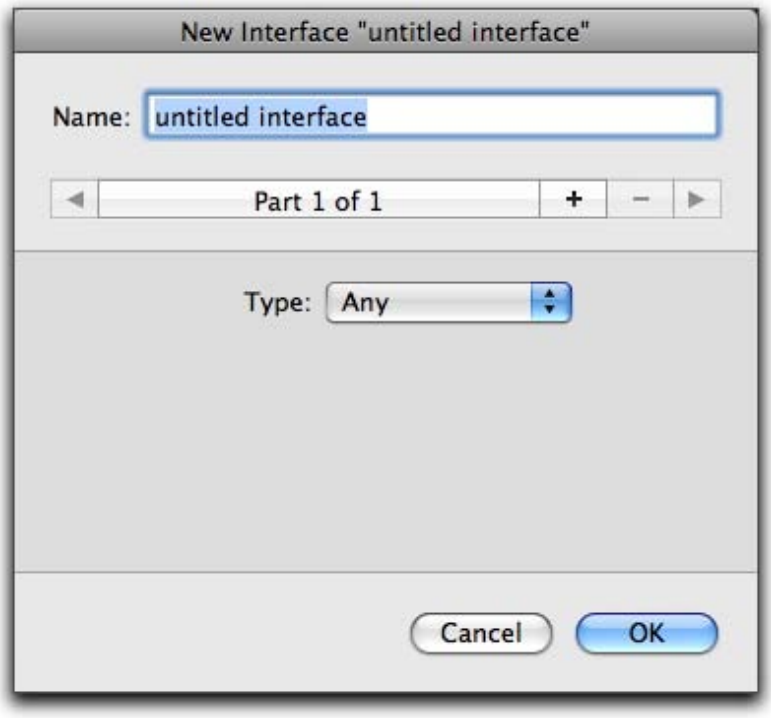
Destination Port is a final option, available only for services utilizing the UDP protocol. If it is checked, packets are filtered according to the function of the Destination Port. If left unchecked, packets are filtered according to the function of the source Port.

Rule Interfaces

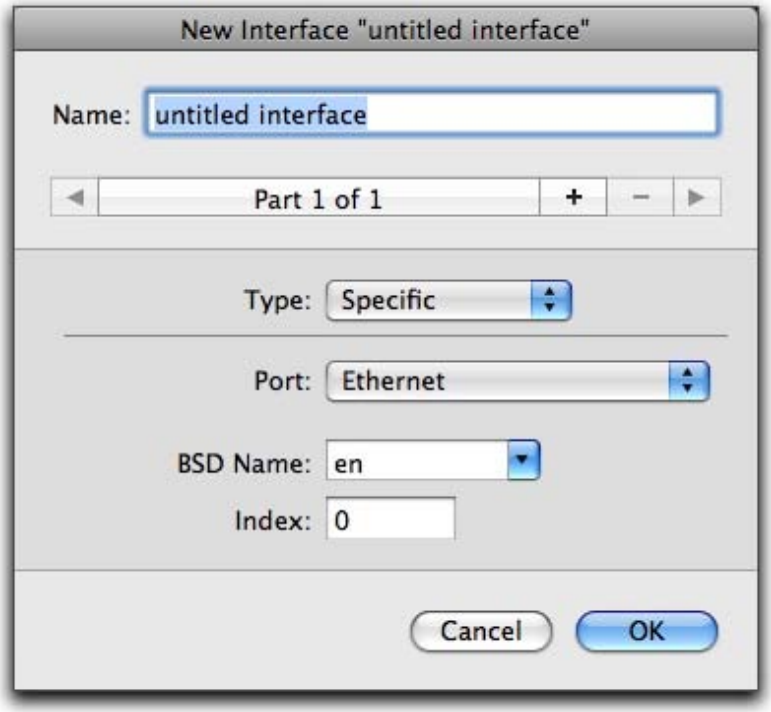
The Interface is the network adapter that the data passes through. This can be an Ethernet card, a wireless AirPort card, or any other type of network interface.

You can choose from a list of preprogrammed interfaces that exist on your computer, or you can create your own interfaces by clicking the + button.

The New Interface editor displays.



The **Type** pop-up menu has two options. The first, **Any**, uses all available network interfaces. The second, **Specific**, lists those interfaces that are available to you, depending on your computer's hardware and software, and gives you some additional options.



Typical interfaces are:

- **Airport**: Wireless networking
- **Built-in Ethernet**: Wired interface commonly used for networking
- **Built-in FireWire**: Wired interface commonly used for peripherals, such as a hard drive, but which can also be used as a network interface

The **BSD Name** and **Index** number are the identifiers used by the Unix layer of Mac OS X. You can set these manually, if you need to. (You probably won't have to, and shouldn't change them if you don't understand what they are.) If other interfaces are present in your Mac, an **Other** option will also be available.

Rule Actions

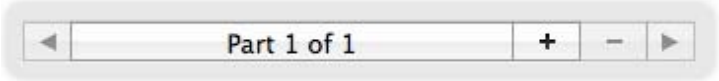
Two actions are possible for any rule: **Allow** or **Deny**. Select the action you wish to use for your rule by checking the appropriate radio button, at the bottom of the Rule Editor window.

Finally, click **OK** to add this rule to your VirusBarrier X6 firewall rules.

Multi-Part Sources, Destinations, Services and Interfaces

Rule sources, destinations, services and interfaces can have several parts. You can, for example, dictate that traffic from several specific IP addresses be banned, listing each one separately in a given Source.

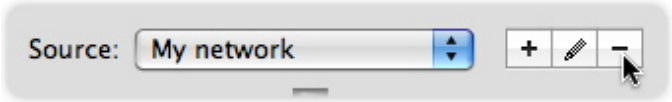
When you create or edit a source, destination, service or interface, you see a bar at the top of the window that looks like this:



- **Create a new part**: Click the + button.
- **Move among parts**: Click the arrow icons. Note that the text in the middle will tell you where you are, and how many parts exist in total. When you reach the last part, clicking the right arrow takes you back to the first one.
- **Delete a part**: To delete a part, it must be visible. Click one of the arrow icons until the part you wish to delete is displayed. Click the - button, then confirm the deletion in the dialog box that follows.

Deleting Sources, Destinations, Services and Interfaces

You can delete any sources that you have created. To do so, select the source, and then click the - button.

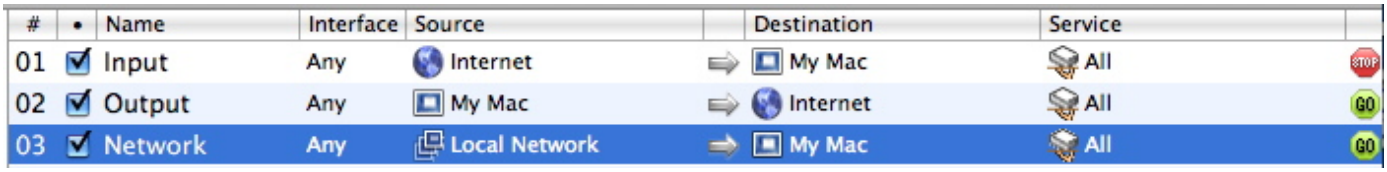


A dialog box displays, asking if you really want to remove that network. Click **Remove** to delete the source network, or **Cancel** if not.

Working with Rules

Rule Order

Rules you add to VirusBarrier X6's firewall are applied from first to last, so you need to make sure that your rules are in the correct order to function properly.



In this example, the first rule blocks data coming from the Internet (which includes all networks, even a local network). Rule 3 allows traffic from a local network; but since it's in 3rd position, it is not applied; the 1st rule takes precedence. For rule 3 to be applied, it needs to be moved to the top of the rule list. To do this, select the rule and drag it to the appropriate position.

Editing and Deleting Rules

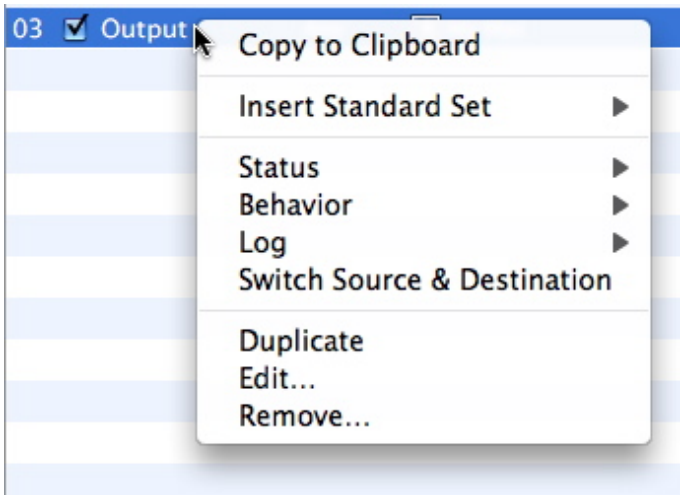
To edit a rule, select the rule by clicking it, then click the button with the pencil icon at the bottom of the list. The Rule Editor will open, and you can make any changes you want to this rule. When you have finished making changes, click **OK** to save your changes. If you decide you do not want to save the changes, click **Cancel**.

To delete a rule, click the rule in the list of rules, then click the - button at the bottom of the list.

Using the Rule Contextual Menu

VirusBarrier X6 lets you make changes to firewall rules quickly through a contextual menu. You can use this contextual menu to add new rules, to edit existing rules, or to change rule characteristics on the fly.

To see this contextual menu, hold down the Control key and click on a rule. (If you have a two-button mouse, you can just click the right button of your mouse.)



The menu offers the following options:

- **Copy to Clipboard**: Copies the contents of a Rule to the Mac's Clipboard in plain-text format. You can then paste the rule into a document, where it will look something like this: "#02/ON/Input/Any/Internet -> My Mac/All/Deny" (where slashes are tabs).
- **Insert Standard Set / Add Standard Set**: Insert or add a standard set of rules, from the same selection as is found in simple mode: No restrictions, No network, Client, Local Server, Server only, or Client only.
- **Status**: You can toggle the state of a rule, turning it On or Off. If the rule is scheduled to run at certain times, a check mark is displayed next to Scheduled in the submenu.
- **Behavior**: Toggle the behavior of a rule between Allow or Deny traffic.
- **Log**: Toggle whether the rule records traffic information in the log.
- **Switch Source & Destination**: "Reverses" a Rule, exchanging the source and destination.
- **Duplicate**: Makes a new copy of the Rule.
- **Edit...**: Opens the Rule Editor for the indicated Rule.
- **Remove...**: Deletes the Rule.

‹‹ VirusBarrier X6 Preferences and Configurations

© 2011 Intego. All Rights Reserved.